Jacobians of Hyperelliptic Curves

Thesis submitted in accordance with the requirements of the
University of Liverpool for the degree of Doctor in Philosophy

John Paul Wunderle

July, 2008

For Isobel and John

Declaration

This dissertation is not substantially the same as any I have submitted for a degree or diploma or other qualification at any other university. Except where indicated in the text, it is the result of my own work and contains nothing which is the outcome of work done in collaboration.

July 2008

Acknowledgements

I wish to thank first my advisor, Prof. E.V. Flynn. Vic has not only been a superlative guide through the world of number theory and its wonderful mysteries, but also a valued friend, in whom I could share my thoughts on a range of topics.

I also wish to thank my family. Without the moral support of my mother, Anne, it would have been impossible to visualise undertaking a PhD (even if there have been rocky times throughout my 3 years!). For your total faith in me, words can not be the tool of expression.

I also wish to thank my uncle, Eric, and aunt, Louise, from whom I have received a great deal of light hearted relief and understanding. Hopefully I have repaid this in kind.

I also wish to honour my friends and colleagues, both in and out of university. Paul (for showing me that friendship is important in life), Shaine (for making me alive to new perceptions of both people and situations), Andy (for telling me what I was and what I am), Tom (for helping shape my outlook to the future and the Dominican Republic), Angela (for letting nothing be complicated), Anthony (for jumping the hurdle and rap), Rachel (for being full of life... thru a lens), Sameer (for showing the grass is greener and improving my chess), Nathan (for accepting your film role and Seth-like outlook), Alana (for help through addiction) and Kieran (for showing the light at the bottom of the well can be sought out). To all those who I have not mentioned, I apologise. So many people have affected my growth in the last 3 years of my research studies. To you all, you have my admiration and respect.

One person who deserves particular praise is Ronnie 'Santa'. Throughout my school life and university education you have been superior to me in so many ways. I aspire to your warmth and outlook.

Finally to Isobel and John, to whom the body is dedicated. I could never have expected any of the array of things you have provided, both materially

and soulfully. You will be together again, Gran and Papa.

I end with a collection of quotations:

"He was crippled. But only his body was cracked. It's not simple, nor is it an easy matter to explain. Let's just leave it at that," she says, and closes the holy book of lies, she covers her eyes, denying to herself what she thought happened. - **Anon.**

It's the story of a lovely lady, who was bringing up three very lovely girls. They all had hair of gold, just like their mother, the youngest one in curls. Its the story, of a man name Brady, who was busy with three boys of his own. It was four men living all together, yet they were all alone. - **Brady Bunch**

Some people live for the fortune, some people live for the fame, some people live for the power, some people live to play the game. Some people think that the physical forms define what is within. I've been there before. That was a bore. So full of the superficial. Some people want it all, I don't want nothing at all, if it ain't you babe, if I ain't got you baby. Some people want diamond rings, some just want everything, but everything means nothing, if I ain't got you! - **Alicia Keys**

Abstract

In this thesis, we look at problems in Number Theory, specifically Diophantine Equations. We investigate Fermat Quartic curves, by presenting a set of methods to determine the existence of rational points on them. We also consider a method of resolving bielliptic curves of genus 2. We show that the method cycles for an infinite family of curves, and find an example where the method fails, however often it is repeatedly applied.

Preface

This work was primarily motivated by examples in the papers [17] and [20]. We investigate problems in Diophantine equations. This subject has a deep history, with a rich body of both proof and conjecture. We consider the arithmetic of curves of genera 1,2 and 3, and combine some of the properties of each type of curve to resolve questions which arise.

In Chapter 1 we set out some of the basic concepts and terminology that will be used throughout. This includes details of Jacobians and their relationship to curves. We also provide some background relating to coverings which will be used in later chapters. As most of this is well known, results are stated, rather than proved explicitly, unless there is something to be gained from understanding the method of proof.

In Chapter 2 we will investigate Fermat Quartic curves of the form

$$x^4 + y^4 = cz^4,$$

which are considered in [20] in response to a challenge of Serre mentioned in [27]. We extend the results in [20], where the authors detail one of the natural covering curves, by giving a description of the two other natural covering curves for c of the form $c = a^4 + b^4$ with $a, b \in \mathbb{Z}$, and provide examples of the most common types at each stage of the process of resolution. We present some numerical data for small values of c at the end of Chapter 2.

Chapter 3 outlines the theory behind the bielliptic isogeny, giving more explicit derivations than there is in the literature. We consider this isogeny, by looking at the kernel and homomorphism properties of the related maps.

Chapters 4,5 deal with covering curves from [17]. We look at possible cycling effects of the algorithm (considered for a special case in [17]). We provide a general version of the method. We also give a family of examples where we show that multiple applications of the method repeat after a finite number of applications, and give a counterexample where the method does not work, however many times the method is repeatedly applied.

Appendix A outlines the idea of 2^{nd} descent.

Contents

Chapter 1

Introduction

1.1 Basic concepts

Here we will outline some of the basic ideas that will be important throughout the future chapters. I have attempted to order the parts of this chapter so that the early concepts relate to early in the thesis, while the later ones relate to the final chapter. However, in order to move seamlessly from topic to topic, it has been essential to have some reordering. We first need to define algebraic varieties, and in particular curves and surfaces.

Definition 1. Let K be a perfect field (that is, every algebraic extension of K is separable) and let $\bar{K}$ be a fixed algebraic closure of K. Let $\mathbb{A}^n(\bar{K})$ and $\mathbb{A}^n(K)$ denote affine n-space over $\bar{K}, K$, respectively. Given any ideal I of $\bar{K}[x_1, \ldots, x_n]$, we let $V_I = \{P \in \mathbb{A}^n(\bar{K}) : f(P) = 0 \text{ for all } f \in I\}$. An (affine) algebraic set is any set of the form V_I for some I. Given an (affine) algebraic set, the *ideal of* V is given by

$$I(V) = \{f \in \bar{K}[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } P \in V\}.$$

We say that V is an (affine) *algebraic variety* if $I(V)$ is a prime ideal in $\bar{K}[x_1, \ldots, x_n]$. Let $\bar{K}(V)$ denote the quotient field of $\bar{K}[x_1, \ldots, x_n]/I(V)$. The *dimension* of an (affine) algebraic variety V is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$. An (affine) *curve* or *surface* is an algebraic variety of

dimension 1 or 2, respectively. We say that an (affine) algebraic set V is *defined over* K if $I(V)$ can be generated by polynomials in $K[x_1, \ldots, x_n]$. When V is defined over K, the set of *K-rational points of V* is the set $V(K) = V \cap \mathbb{A}^n(K)$.

We can similarly define projective versions of the above definitions.

Definition 2. Let K be as in Definition 1 and let $\mathbb{P}^n(\bar{K})$ and $\mathbb{P}^n(K)$ denote projective n-space over $\bar{K}, K$, respectively. We say that a polynomial $f \in \bar{K}[X_0, \ldots, X_n]$ is *homogeneous of degree d* if $f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$ for all $\lambda \in \bar{K}$. We say that an ideal I of $\bar{K}[X_0, \ldots, X_n]$ is *homogeneous* if it is generated by homogeneous polynomials. Given any homogeneous ideal I of $\bar{K}[X_0, \ldots, X_n]$, we let

$$V_I = \{P \in \mathbb{P}^n(\bar{K}) : f(P) = 0 \text{ for all homogeneous} f \in I\}.$$

A (projective) algebraic set is any set of the form V_I for some homogeneous I. Given a (projective) algebraic set, the *ideal of V* is the ideal in $\bar{K}[X_0, \ldots, X_n]$ generated by

$$\{f \in \bar{K}[X_0, \ldots, X_n] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}.$$

We say that V is a (projective) *algebraic variety* if $I(V)$ is a prime ideal in $\bar{K}[X_0, \ldots, X_n]$. Take any choice of $\mathbb{A}^n(\bar{K}) \subset \mathbb{P}^n(\bar{K})$ such that $V \cap \mathbb{A}^n(\bar{K}) \neq \emptyset$; then the *dimension* of the projective algebraic variety V is defined to be the dimension of the affine algebraic variety $V \cap \mathbb{A}^n(\bar{K})$. A (projective) *curve* or *surface* is a (projective) algebraic variety of dimension 1 or 2, respectively. We say that a (projective) algebraic set V is *defined over K* if $I(V)$ can be generated by polynomials in $K[X_0, \ldots, X_n]$. When V is defined over K, the set of *K-rational points of V* is the set $V(K) = V \cap \mathbb{P}^n(K)$.

We shall typically describe an algebraic variety V by providing a specific set of defining equations for $I(V)$, and say that V is given by (or defined by) these equations. All of the curves in this thesis are taken to be projective curves, even though we sometimes use affine equations $f_i(x_1, \ldots, x_n)$ as a

shorthand notation for their homogenisation (the equations $F_i(X_0, \ldots, X_n)$ of the same degree, such that $F_i(1, x_1, \ldots, x_n) = f_i(x_1, \ldots, x_n)$). A curve $F(X, Y, Z) = 0$ is *smooth* if there does not exist a point $P \in \mathbb{P}^2(\bar{K})$ at which $F(P) = \frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$. A *point at infinity* on the curve will be a point on the projective curve with $Z = 0$. We assume that all of our projective curves are smooth. We shall mainly be dealing with curves of genus 1 and 2. We shall not give a definition of genus here; the form of our curves will typically be in the hyperelliptic form $\mathcal{C} : Y^2 = F(X)$, where $F(X)$ has degree $d = 3, 4, 5, 6$ and has nonzero discriminant. This has genus 1 when $d = 3, 4$ (see Prop. 3.1(c) in Chapter III of [29] and p.35 of [6]) and has genus 2 when $d = 5, 6$ (p.322 of [23]). There are no singular points on $Y^2 = F(X)$ when $d = 3$; there is a singular point at infinity when $d = 4, 5, 6$. Recall that we shall always mean the corresponding projective smooth curve (see equation 1.1.5 on p.2 of [8] for an explicit set of defining equations). When d is odd, the point at infinity on $Y^2 = F(X)$ corresponds to one K-rational point on the projective smooth model, which we'll call ∞, and which will always be a member of $\mathcal{C}(K)$. When d is even, the point at infinity on $Y^2 = F(X)$ corresponds to two points on the projective smooth model (the two 'branches' at infinity), which we'll call ∞^+ and ∞^-; these are in $\mathcal{C}(K)$ exactly when the leading coefficient of $F(X)$ is in $(K^*)^2$.

In summary, when we write a curve $\mathcal{C} : Y^2 = F(X)$, where $F(X)$ is of degree 3,4,5,6 and has nonzero discriminant, then this is a shorthand notation for the corresponding projective smooth curve, and the points in $\mathcal{C}(K)$ will be: the affine points (x, y) [where $x, y \in K$ satisfy $y^2 = F(x)$], together with ∞ [when d is odd] and ∞^+, ∞^- [when d is even and the leading coefficient of $F(X)$ is in $(K^*)^2$].

Definition 3. For any field K, we say that $v : K \to \mathbb{R} \cup \{\infty\}$ is a *valuation* if:

$$v(a) = \infty \iff a = 0, \quad v(ab) = v(a) + v(b) \text{ for all } a, b \in K^*, \text{ and}$$

$$v(a + b) \geq \min\big(v(a), v(b)\big).$$

Given any valuation v, there is a corresponding absolute value $|\ |_v$ defined by $|a|_v = \rho^{v(a)}$, where ρ is any fixed real number satisfying $0 < \rho < 1$. Then $|\ |_v : K \to \mathbb{R}$ satisfies:

$$|a|_v = 0 \iff a = 0, \quad |ab|_v = |a|_v|b|_v, \text{ and } |a+b|_v \leq \max(|a|_v, |b|_v).$$

The *completion* of K with respect to v, denoted K_v, is the smallest field containing K which is complete with respect to $|\ |_v$. It is formally constructed as the set of Cauchy sequences in K modulo the equivalence relation that (a_n) and (b_n) are equivalent if and only if $|a_n - b_n|_v \to 0$. It is easy to check (see, for example, Chapter 2 of [5]) that this is a field, that it contains a copy of K, that the field operations of K can be extended to K_v and that the valuation v can be extended to K_v.

Definition 4. A curve, defined over a number field K, is said to be *everywhere locally solvable* if it has points in every completion of K.

Since we are working primarily in $\mathbb{Q}$, this means our curves will be everywhere locally solvable if there are points in every $\mathbb{Q}_p$ and $\mathbb{R}$, where $\mathbb{Q}_p$ are the field of p-adic numbers. We recall what is meant by $\mathbb{Q}_p$.

Definition 5. Let p be a fixed prime and t some rational number, then we can write t as

$$t = p^r \frac{a}{b}, r, a, b \in \mathbb{Z}$$

and where p does not divide into a or b. We have a valuation $v_p(t) = r$ and the p-adic absolute value of t is

$$|t|_p = p^{-v_p(t)}.$$

The *p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to this valuation.

Much of our work will involve the Picard group. We recall from the definition on p.32 of [29] that $\mathrm{Pic}^0(\mathcal{C})$ is the group of divisors $D = \sum_{P \in \mathcal{C}} n_P P$, with $n_P \in \mathbb{Z}$, $n_P = 0$ for all but finitely many $P \in \mathcal{C}$ and $\sum_{P \in \mathcal{C}} n_P = 0$, modulo linear equivalence (the divisors of functions on the curve); furthermore,

$\mathrm{Pic}^0_K(\mathcal{C})$ is the subgroup of $\mathrm{Pic}^0(\mathcal{C})$ fixed by all Galois action from $\bar{K}$ to K. An *abelian variety* is a projective variety with the structure of an abelian group such that the multiplication and inverse maps are morphisms of projective varieties. Associated to any curve is also the *Jacobian* (variety) J, which is an abelian variety of dimension g. As a group, $J(K)$ is isomorphic to $\mathrm{Pic}^0_K(\mathcal{C})$. The *genus* of a curve can be defined as the dimension of its Jacobian variety. In genus 2, an explicit set of defining equations is given in [8] via a "blowing down" process, described fully in [25] and [32]. We shall not be making any use of the structure of the Jacobian as an algebraic variety, and we only require the Mordell-Weil group $J(K)$ of K-rational points on the Jacobian which, as we have noted, is the same as $\mathrm{Pic}^0_K(\mathcal{C})$. Furthermore, we shall not require the fine details of the general definition of $\mathrm{Pic}^0_K(\mathcal{C})$ (such as linear equivalence), since we shall only deal explicitly with the group law in two cases: genus 1 and genus 2, where there are well known ways of describing $J(K)$ and the group law. Any curve of genus 1 or 2 can be written in *hyperelliptic form*: $y^2 = f(x)$.

For a curve of genus 1, the Jacobian J is an elliptic curve, and so J can be written as a smooth cubic curve. In this case, the group law is just given by the standard construction (as on p.55 of [29]), that three points sum to the identity when they are collinear. For genus 2, we have the following explicit description (see Chapter 8 of [8]).

Example 1. Let us consider the genus 2 case. Let

$$\mathcal{C} : y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

defined over some field K of characteristic zero, where the discriminant is non-zero, represent a general genus 2 curve. When $f_6 \neq 0$, we use ∞^+, ∞^- to denote the points on the smooth curve that lie over the singular point at infinity on $\mathcal{C}$. When $f_6 = 0$ and so $f_5 \neq 0$, we let ∞ denote the point at infinity. Any member of $J(K)$, the K-rational points on the Jacobian, is represented by a divisor of the form $P_1 + P_2 - \infty^+ - \infty^-$ (or $P_1 + P_2 - 2\infty$), where P_1, P_2 are points on $\mathcal{C}$ (possibly repeated) and either they are both K-rational or are quadratic over K (and conjugate). It is often convenient

to abbreviate such a divisor as $\{P_1, P_2\}$, which gives a 1-1 correspondence with members of $J(K)$, except that all sets of the form $\{(x, y), (x, -y)\}$ should be identified as $\mathcal{O}$, the identity element of $J(K)$. Three members $\{P_1, P_2\}$, $\{Q_1, Q_2\}$, $\{R_1, R_2\} \in J(K)$ sum to $\mathcal{O}$ when there is a function $Y =$ cubic in X through $P_1, P_2, Q_1, Q_2, R_1, R_2$ (with straightforward adjustments for special cases, such as repeated points).

The following Theorem is known as the Mordell-Weil Theorem and is proved, for example, in [34].

Theorem 1. *Consider a curve of genus g defined over a number field K with Jacobian J. Let $J(K)_{tor}$ denote the subgroup of elements of $J(K)$ of finite order. Then $J(K)$ is finitely generated and so:*

$$J(K) \approx J(K)_{tor} \times \mathbb{Z}^r.$$

We say that r is the rank of $J(K)$.

There are a number of different ways we can tackle the calculation of the rank. The main ways to attack this problem involve a method known as descent. Briefly, this process involves looking at some associated algebraic varieties, known as homogeneous spaces. We have a set of these to consider. If they do not have points in every local completion then we can eliminate them from the process. As described, for example in Chapter 11 of [8], there is an injection $q : J(K)/2J(K) \rightarrow M$, where M is a known finite subgroup of a cartesian product of the multiplicative groups of the nonzero elements of number fields, modulo squares. Note that, if we have computed $J(K)_{tor}$ then we can deduce the rank from $J(K)/2J(K)$, using $J(K)/2J(K) \approx J(K)_{tor}/2J(K)_{tor} \times (\mathbb{Z}/2\mathbb{Z})^r$. The question of whether a given $d \in M$ is in the image of q is equivalent to deciding whether an associated space H_d has a K-rational point. We can bound the size of $J(K)/2J(K)$ [and hence the rank r] by finding all $d \in M$ such that H_d has points defined over every completion of K. We shall refer to this as the 2-*Selmer bound* on the rank of $J(K)$ (see Chapter 11 of [8] for further details of this process). Problems occur when there are points in every completion, but still there

are no K-rational points. This is known as *failure of the Hasse principal.* We shall not focus on these methods of descent, however they are described completely in [29],[30] and [38] – the latter implementing an idea of 2^{nd} descent which is outlined in Appendix A. There are various programs (for example [38],[40]) which compute the 2-Selmer bound on the rank of elliptic curves and the Jacobians of curves of genus 2.

The following conjecture will be applied in some cases when, even though we have been unsuccessful in finding the rank of a curve, we have still found an upper bound on the 2-Selmer bound on the rank. The following parity conjecture can be found in many sources, such as [6] and is used in the computer package [38].

Conjecture 1. *Let J be the Jacobian of a curve, defined over a number field K. If the 2-Selmer bound on the rank of $J(K)$ is even, then the actual rank is even; if the 2-Selmer bound on the rank is odd, then the actual rank is odd.*

Let A_1, A_2 be abelian varieties. A *morphism* of abelian varieties $\phi : A_1 \to A_2$ is a morphism of projective varieties which is also a group homomorphism. Such a morphism ϕ is an *isogeny* if it is surjective and has a finite kernel. We say that A_1 and A_2 are *isogenous* if there exists an isogeny from A_1 to A_2; one can check that isogeny is an equivalence relation. An abelian variety is *reducible* if it is the product of two abelian varieties of positive dimension.

1.2 A detailed look at Jacobians and covers

In this section we will look a bit more into how a Jacobian relates to a curve, and how covers can be used to relate questions about finding $\mathcal{C}(K)$ to that of finding rational points on associated collections of curves.

1.2.1 The Abel-Jacobi Map

Suppose that a curve $\mathcal{C}$ is defined over K. Recall that, as a group, $J(K)$ is isomorphic to $\mathrm{Pic}^0_K(\mathcal{C})$. Suppose that $\mathcal{C}(K)$ is nonempty, and that we

fix a point $P_0 \in \mathcal{C}(K)$. Then $P \mapsto [P - P_0]$ (the divisor class containing $P - P_0$) is an injection of $\mathcal{C}(K)$ into $J(K)$. When $\mathcal{C}$ has genus 2, note that $[P-P_0] = [P+Q_0-\infty^+-\infty^-] = \{P, Q_0\}$, in the notation of Example 1, where Q_0 is the image of P_0 under the hyperelliptic involution $(x, y) \mapsto (x, -y)$.

1.2.2 Covers of Curves

Most of this background in covers is from the beginning of Chapter 2 of [33], however I have chosen to limit the theory to that over $\mathbb{Q}$, rather than a general number field K as the author in [33] deals with, since in this thesis all covers will be over $\mathbb{Q}$.

Definition 6. Let $\mathcal{C}$ be a curve defined over $\mathbb{Q}$ with a Jacobian, J. A *cover* of $\mathcal{C}$ is a surjective map from a curve $\mathcal{D}$ onto $\mathcal{C}$. We say that the cover $\mathcal{D} \to \mathcal{C}$ *hits* the point $P \in \mathcal{C}(\mathbb{Q})$ if P is in the image of $\mathcal{D}(\mathbb{Q})$.

We also require the idea of a collection of these covers since one single $\mathcal{D}$ may not hit all points of $\mathcal{C}$.

Definition 7. Let $\mathcal{C}$ be a curve defined over $\mathbb{Q}$ with a Jacobian, J. Then we define a *covering collection* for $\mathcal{C}$ over $\mathbb{Q}$ to be a set $\{\mathcal{D}_i \to \mathcal{C}\}$ of $\mathbb{Q}$-rational covers of $\mathcal{C}$ in a single isomorphism class, such that every point of $\mathcal{C}(\mathbb{Q})$ is hit by a point in some $\mathcal{D}_i(\mathbb{Q})$.

The problem of finding the set of rational points on $\mathcal{C}$ becomes instead the problem of finding the rational points on each of the covers. One method for obtaining covers is by using an isogeny defined over $\mathbb{Q}$, from an Abelian variety A to the Jacobian J. Suppose we are given an abelian variety A, defined over $\mathbb{Q}$, and a $\mathbb{Q}$-rational isogeny $\phi : A \to J$ of degree d (that is, the kernel has order d). Suppose also that $P_0 \in \mathcal{C}(\mathbb{Q})$ and that we have computed $J(\mathbb{Q})/\phi(A(\mathbb{Q})) = \{D_1, \ldots, D_n\}$. Let $\mathcal{C}_i$ be the image of $\mathcal{C}$ in J under the embedding $P \mapsto [P - P_0] - D_i$, and let $\mathcal{D}_i$ be the pullback of $\mathcal{C}_i$ to A via ϕ. Then Theorem 3.3 of [33] shows that $\mathcal{D}_i$ is a covering collection for $\mathcal{C}$; in order to find $\mathcal{C}(\mathbb{Q})$, it is sufficient to find every $\mathcal{D}_i(\mathbb{Q})$.

Chapter 2

Fermat Quartics

The Fermat quartic curves $aX^4 + bY^4 = cZ^4$ and, in particular, the special cases

$$\mathcal{D}_c : X^4 + Y^4 = cZ^4,$$

for $c \in \mathbb{Z}$, not divisible by the fourth power of a prime, have been studied, for example, in [10],[27],[20]. In [20], the authors solve a problem first mentioned by Serre in [27]. The problem concerns the number of rational points on the curve

$$\mathcal{D}_{17} : \ X^4 + Y^4 = 17Z^4,$$

i.e. the case when $c = 17$. They use covering techniques to solve the problem. We will consider a method which attempts to decide whether the general form of $\mathcal{D}$ has rational points, and then go on to specialise for when we have a guaranteed rational point, and see how we can attempt to find all the rational points. Also, we will often switch between the projective form and the affine form where the meaning is obvious from the context.

2.1 Approaches to finding rational points on the curve $\mathcal{D}$

The first approach to finding the rational points on $\mathcal{D}$ is to ensure the curve has points in every local field. Since we are looking for points in $\mathbb{Q}$, this

involves ensuring that there are points in every $\mathbb{Q}_p$ and $\mathbb{R}$. This will eliminate some of the c.

Example 2. Consider the case $c = 3$. The curve $X^4 + Y^4 = 3$ has no point in $\mathbb{Q}_5$. So immediately we have that there are no $\mathbb{Q}$-rational points.

Proof. Let $X, Y \in \mathbb{Q}_5$ satisfy $X^4 + Y^4 = 3$. First consider the case when $|X|_5, |Y|_5 \leq 1$. Then $X^4 \equiv 0, 1$ and $Y^4 \equiv 0, 1$ modulo 5, and so $X^4 + Y^4 \neq 3$.

If either $|X|_5$ or $|Y|_5$ is > 1 then we must have $|X|_5 = |Y|_5$ (since otherwise $|X^4 + Y^4|_5$ would equal the maximum of $|X^4|_5$ and $|Y|_5$ and so could not equal $|3|_5 = 1$), say that $|X|_5 = |Y|_5 = 5^k$ for some $k > 0$. Then we can write $X = a/5^k, Y = b/5^k$ for some a, b with $|a|_5 = |b|_5 = 1$. Then $a^4 + b^4 = 3 \cdot 5^{4k} \equiv 0$ modulo 5. But $a^4 \equiv b^4 \equiv 1$ modulo 5, a contradiction. ∎

Clearly the same argument rules out any $c \equiv 3 \pmod 5$. Recall from Section 1 of [20], where local considerations give that: any odd prime p dividing c must satisfy $p \equiv 1 \pmod 8$; furthermore $c \equiv 1, 2 \pmod{16}$, $c \not\equiv 3, 4 \pmod 5$, $c \not\equiv 7, 8, 11 \pmod{13}$, $c \not\equiv 4, 5, 6, 9, 13, 22, 28 \pmod{29}$.

The next approach is natural, in that we consider the Jacobian of $\mathcal{D}$, which we denote $J(\mathcal{D})$. This Jacobian is reducible, and in fact is isogenous to the product of elliptic curves. We have a Jacobian of dimension 3. We can take advantage of the fact that there are the maps

$$\omega_1 : (X, Y, Z) \mapsto (X^2, YZ, Z^2), \ \omega_1' : (X, Y, Z) \mapsto (Y^2, XZ, Z^2)$$

from $\mathcal{D}$ to the genus 1 curve $\mathcal{F}_1$, and the map

$$\omega_2 : (X, Y, Z) \mapsto (X^2, XY, Z^2)$$

from $\mathcal{D}$ to the genus 1 curve $\mathcal{F}_2$, where

$$\mathcal{F}_1 : X^2Z^2 + Y^4 = cZ^4,$$

$$\mathcal{F}_2 : X^4 + Y^4 = cX^2Z^2,$$

which in turn have respective Jacobians given, up to isogeny, by the elliptic curves

$$\mathcal{E}_1 : y^2z = x^3 - cxz^2,$$

$$\mathcal{E}_2 : y^2z = x^3 + c^2xz^2.$$

There are two ways we can verify this. One way is to construct 2-to-1 maps ρ_1 from $\mathcal{F}_1$ to $\mathcal{E}_1$ and ρ_2 from $\mathcal{F}_2$ to $\mathcal{E}_2$, given by

$$\rho_1 : (X, Y, Z) \mapsto (-Y^2, XY, Z^2),$$

$$\rho_2 : (X, Y, Z) \to (cY^2, c^2YZ, X^2).$$

Each ρ_i (for $i = 1, 2$) induces a 2-isogeny of Jacobians, given by $[\sum P] \mapsto [\sum \rho_i(P)]$, where [ ] denotes divisor class modulo linear equivalence. The kernel, for the case $i = 1$ is given by the identity and $[(0, \gamma, 1) - (0, -\gamma, 1)]$, where γ is a fixed fourth root of c (which is a point of order two on the Jacobian of $\mathcal{F}_1$; note that the other choices of γ merely give other representatives of the same divisor class). Similarly the kernel, for the case $i = 2$ is given by the identity and $[(1, \gamma', 0) - (1, -\gamma', 0)]$, where γ' is a fixed fourth root of -1. In any case, we shall not make any use of the fact that the above maps are 2-isogenies; the important comment is that, for $i = 1, 2$, any rational point on $\mathcal{F}_i$ gives a rational point on $\mathcal{E}_i$, and that the map induced on the Jacobian by the rational map is an isogeny, and so the rank of $\mathcal{E}_i$ is the same as the rank of the Jacobian of $\mathcal{F}_i$. Note that, given a point (U, V, W) on $\mathcal{E}_1$ it is easy to find all of the preimages on $\mathcal{F}_1$, since $-Y^2 = U, XY = V, Z^2 = W$ gives $(Y/Z)^2 = -U/W$ and so only two choices for the ratio Y/Z; also, $X/Y = -V/U$ is fixed, and so there are only two possibilities for the preimage (X, Y, Z), showing that ρ_1 is a 2-to-1 map from $\mathcal{F}_1$ to $\mathcal{E}_1$. Similarly, given a point (U, V, W) on $\mathcal{E}_2$ it is easy to find all of the preimages on $\mathcal{F}_2$, since $cY^2 = U, c^2YZ = V, X^2 = W$ gives $(X/Y)^2 = cW/U$ and so only two choices for the ratio X/Y; also, $Y/Z = cU/V$ is fixed, and so there are only two possibilities for the preimage (X, Y, Z), showing that ρ_2 is a 2-to-1 map from $\mathcal{F}_2$ to $\mathcal{E}_2$. It is similarly easy to find preimages under the maps $\omega_1 : \mathcal{D} \to \mathcal{F}_1$, $\omega_1' : \mathcal{D} \to \mathcal{F}_1$ and $\omega_2 : \mathcal{D} \to \mathcal{F}_2$.

The other way is to use Weil's Method from [35] where the author gives a formula for calculating the Weierstrass form of the Jacobian;

$$\mathcal{C} : y^2 = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4,$$

has Jacobian

$$J : \zeta^2 = 4\xi^3 - i\xi - j,$$

$$i = a_0a_4 - 4a_1a_3 + 3a_2^2,$$

$$j = a_0a_2a_4 + 2a_1a_2a_3 - a_0a_3^2 - a_4a_1^2 - a_2^3.$$

So, for our $\mathcal{F}_1$, we "choose" Z to go to $Z = 1$ to put us into affine form, and for our $\mathcal{F}_2$, we "choose" X to go to $X = 1$ to put us into affine form (and divide through by c) to get $\mathcal{F}_1, \mathcal{F}_2$ in affine form as:

$$X^2 = -Y^4 + c,$$

$$Z^2 = \frac{1}{c}Y^4 + \frac{1}{c},$$

which are in the required form to use Weil's formula (on replacing 'y' with X and 'x' with Y for $\mathcal{F}_2$, and replacing 'y' with Z and 'x' with Y for $\mathcal{F}_2$). In the case of $\mathcal{F}_1$ we will have $a_0 = -1, a_4 = c$, and $a_1 = a_2 = a_3 = 0$, and so (from Weil's formula) $i = -c, j = 0$. In the case of $\mathcal{F}_2$ we will have $a_0 = a_4 = \frac{1}{c}$, and $a_1 = a_2 = a_3 = 0$ and so (from Weil's formula) $i = 1/c^2, j = 0$. Substituting these into Weil's formula gives that the Jacobians of $\mathcal{F}_1, \mathcal{F}_2$ are

$$J_1 : \zeta^2 = 4\xi^3 + c\xi,$$

$$J_2 : \zeta^2 = 4\xi^3 - \frac{1}{c^2}\xi,$$

respectively. Now note that, taking $x = 4\xi, y = 4\zeta$ transforms J_1 to

$$J_1' : y^2 = x^3 + 4cx,$$

and that $\mathcal{E}_1$ is 2-isogenous to J_1' under the standard 2-isogeny (see, for example, p.302 of [29]) from any curve of the form $y^2 = x^3 + Ax^2 + Bx$ to

$y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x$.

Similarly, taking $x = 4c^2\xi, y = 4c^3\zeta$ transforms J_2 to

$$J_2' : y^2 = x^3 - 4c^2x,$$

and that $\mathcal{E}_2$ is 2-isogenous to J_2' under the same standard 2-isogeny.

One can check that the pull backs of the regular differentials on $\mathcal{E}_1$ and $\mathcal{E}_2$ are linearly independent on $J(\mathcal{D})$, for which it is sufficient to show that the pullbacks to $\mathcal{D}$ are linearly independent, as has been done on p.67 of [27]. Therefore we have that $J(\mathcal{D})$ is isogenous to the product of 3 Jacobians above, given by the elliptic curves stated. We can write

$$J(\mathcal{D}) \approx \mathcal{E}_1 \times \mathcal{E}_1 \times \mathcal{E}_2.$$

Whenever we have Mordell-Weil rank of 0 for $\mathcal{E}_i(\mathbb{Q})$ for either $i = 1$ or $i = 2$, then we can compute the preimages on $\mathcal{D}$ under $\omega_i \circ \rho_i$ of the members of $\mathcal{E}_i(\mathbb{Q})$. This will be a finite set of points on $\mathcal{D}$, and we can inspect which of these are rational in order to find $\mathcal{D}(\mathbb{Q})$.

Example 3. Consider the value $c = 2$. The curve $\mathcal{D} : X^4 + Y^4 = 2Z^4$ has points in every $\mathbb{Q}_p$ and $\mathbb{R}$. We can also see that there are 4 obvious points, namely $(1, \pm 1, \pm 1)$. It is relatively simple to show that these are all possible rational points, as follows. Taking $\mathcal{E}_2$ for this value of c gives the elliptic curve $y^2z = x^3 + 4xz^2$. It is quite a simple process (which we have checked using [38]) to show that $\mathcal{E}_2(\mathbb{Q})$ has rank 0 and that the list of torsion points is $\{(0,1,0), (0,0,1), (2, \pm 4, 1)\}$. Composing the maps $\omega_2 : \mathcal{D} \to \mathcal{F}_2$ and $\rho_2 : \mathcal{F}_2 \to \mathcal{E}_2$ gives the 4-to-1 map

$$\rho_2 \circ \omega_2 : \mathcal{D} \to \mathcal{E}_2 : (X, Y, Z) \mapsto (cX^2Y^2, c^2XYZ^2, X^4) = (cXY^2, c^2YZ^2, X^3).$$

The point $(0,1,0) \in \mathcal{E}_2(\mathbb{Q})$ has preimages $(0, \pm\gamma, 1), (0, \pm i\gamma, 1)$ on $\mathcal{D}$, where γ is any fixed choice of fourth root of 2; none of the points are defined over $\mathbb{Q}$. Similarly, the point $(0,0,1) \in \mathcal{E}_2(\mathbb{Q})$ has preimages $(\pm\gamma, 0, 1), (\pm i\gamma, 0, 1)$ on $\mathcal{D}$, and again none of these points are defined over $\mathbb{Q}$. Finally, the points $(2, \pm 4, 1) \in \mathcal{E}_2(\mathbb{Q})$ have preimages $(1, \pm 1, \pm 1), (1, \pm 1, \pm i)$ on $\mathcal{D}$, and only

$(1, \pm 1, \pm 1)$ are defined over $\mathbb{Q}$. We have shown therefore that $X^4+Y^4 = 2Z^4$ has only the obvious rational points $(1, \pm 1, \pm 1)$.

It is interesting to note how important a role $\mathcal{F}_1$ plays. The following lemma shows its occurrence as a homogeneous space for $\mathcal{E}_1$, and in fact it is the most "crucial" homogeneous space that requires consideration.

Lemma 1. *Consider the genus 1 curve $\mathcal{F}_1 : X^2Z^2 + Y^4 = cZ^4$, which has Jacobian isogenous to $\mathcal{E}_1 : y^2 = x(x^2-cz^2)$. Then $\mathcal{F}_1$ occurs as a homogeneous space of $\mathcal{E}_1$. Since all rational points on $\mathcal{D}$ are mapped to points on $\mathcal{F}_1$, then if $\mathcal{F}_1(\mathbb{Q}) = \phi$ we have $\mathcal{D}(\mathbb{Q}) = \phi$.*

Proof. The second part of this, namely that if $\mathcal{F}_1(\mathbb{Q}) = \phi$ we have $\mathcal{D}(\mathbb{Q}) = \phi$, is obvious. To show the fact that $\mathcal{F}_1$ occurs as a homogeneous space, recall (see p.63 of [6]) that for a general elliptic curve of the form $y^2 = x(x^2+ax+b)$, a homogeneous space of this curve is the locally solvable quartic $rv^4 + av^2 + \frac{b}{r} = u^2$, where $r|b$. Our curve, $\mathcal{E}_1$, is, in affine form, $y^2 = x^3 - cx = x(x^2 - c)$. So this curve has homogeneous spaces of the form $rv^4 + \frac{-c}{r} = u^2$, where $r|-c$. Clearly we will have $r = -1$ as a homogeneous space. This will be the equation $-v^4 + c = u^2$, which is an affine form of $\mathcal{F}_1$. ∎

The next logical approach is to consider higher ranks. If the curve $\mathcal{E}_1$ has rank 1, then there is a method of Dem'janenko and Manin (mentioned in [10]) which is applicable when the rank of the group of morphisms of $\mathcal{D}$ into some elliptic curve exceeds the rank of this elliptic curve. This case is extremely rare, and in cases I have found where this might be applicable, it is possible to use a 2^{nd} descent (as outlined in Appendix A).

Example 4. We will consider the example $c = 2642$. This is the first example of its type, where we have to use second descents (as outlined in Appendix A) to show that $\mathcal{F}_1(\mathbb{Q}) = \phi$, which in turn shows that $\mathcal{D}(\mathbb{Q}) = \phi$. Doing a normal descent via isogeny, we find that the homogeneous space of $y^2 = x(x^2 - 2642)$ which is $\mathcal{F}_1$, can not be resolved by either $\mathbb{Q}_p$ or $\mathbb{R}$ arguments, that the rank is bounded above by 3, and that the rank being 1 would imply that this homogeneous space would have no rational points. So, we can apply the 2^{nd}

descent as outlined in Appendix A to resolve this space (which has equation $-v^4 + 2642 = u^2$). Note that [38] computes the rank as 1, and proves after a second descent that $-v^4 + 2642 = u^2$ has no rational points. The techniques for these ranks are entirely standard elliptic curves techniques, and are all obtained by commands in standard packages, such as Apecs [38].

As stated, it is also possible to apply the method of Manin-Dem'janenko (for instance if 2^{nd} descent was unsuccessful), however this is extremely rare and of all cases I have checked (with $c \leq 20000$) at no time was this method required. For completeness, it is worthwhile to briefly mention it. We start with a curve and consider when this curve admits morphisms into some elliptic curve(s) (as our $\mathcal{D}_c$ does). If the rank of this group of morphisms exceeds the rank of the curve then the method can be applied. This can produce a very effective upper bound on the heights of rational points on our original curve. Unfortunately the Fermat quartics we are looking at do not allow use of this technique.

Another such bounding technique is presented in the following classical result of Chabauty [9]

Theorem 2. *Let $\mathcal{C}$ be a curve of genus g defined over a number field K, whose Jacobian has Mordell-Weil rank $\leq g - 1$. Then $\mathcal{C}$ has only finitely many points.*

Of course, the result is known to be unconditionally true (with no condition on the rank) by Falting's Theorem [11], but Chabauty's method gives an explicit bound on the total number of rational points of a curve, which often turns out in practice to be sharp (see [15]). The argument is p-adic and each value of p produces a different bound so there are effectively infinitely many chances of applying the technique. There are also practical techniques in the literature (such as [15]), which describe explicitly how to use Chabauty's Theorem to obtain bounds on the number of rational points. As our curves $\mathcal{D}_c$ are genus 3 (since it is a smooth plane quartic, and any smooth plane curve of degree d has genus $(d-1)(d-2)/2$; see pages 41,43 of [29]), Chabauty is directly applicable to the curve $\mathcal{D}_c$ only when the rank

is ≤ 2. However since $J(\mathcal{D}_c)$ is isogenous to $\mathcal{E}_1 \times \mathcal{E}_1 \times \mathcal{E}_2$ as above, this is equivalent to $\mathcal{E}_1$ having rank 0 or $\mathcal{E}_2$ having rank 0 while $\mathcal{E}_1$ has rank 1.

So if we were to list values of c, we have some machinery with which we can treat these cases. If at first local considerations are unsuccessful at resolving then we can attempt a number of methods by considering maps to various genus 1 curves. However not all the curves will have the required ranks low enough. In the next section we will investigate how we can proceed if we know for certain that we have at least one rational point on $\mathcal{D}$.

2.2 A covering approach for $c = p = a^4 + b^4$ where p is prime

In [8], associated curves of genus 5 and 2 are found, and it is shown that it is sufficient to find the rational points on the curves of genus 2 in order to find $\mathcal{D}(\mathbb{Q})$. This was used in [20] to solve the case $p = 17$. We will present the other two covers for $c = p = a^4 + b^4$ where p is a prime, which have not previously been described.

2.2.1 Covering curves

From [20] the authors find a curve of genus 5 which covers a curve of genus 2 of the form

$$y^2 = G_1(x)G_2(x)G_3(x),$$

where

$$G_1(x) = (a+b)^2x^2 - 4(a^2+ab+b^2)x + 2(a+b)^2,$$

$$G_2(x) = (a-b)^2x^2 + 4(a^2-ab+b^2)x + 2(a-b)^2,$$

$$G_3(x) = x^2 - 2.$$

We will imitate the methods in [20] to obtain the other covers.

2.2.2 Second cover

As before, suppose that $c = p = a^4 + b^4$ where p is a prime, and that $(X, Y, Z) \in \mathcal{D}$, where $X, Y, Z \in \mathbb{Z}$ and we have removed any nontrivial common factors, so that the highest common factor of X, Y, Z is 1.

We can write the general form of the curve $\mathcal{D}$ as

$$\{(cZ^2 + \phi_1(X,Y))(cZ^2 - \phi_1(X,Y))\} = \phi_2(X,Y)^2, \tag{2.1}$$

where

$$\phi_1 = (a^2X^2 + b^2Y^2),$$

$$\phi_2 = (a^2Y^2 - b^2X^2).$$

The 2 factors on the LHS of the above equation do not have any common zeros on our curve $\mathcal{D}$. We can therefore write as a double cover a pair of equations

$$(cZ^2 + \phi_1(X,Y)) = dR^2,$$

$$dR^2(cZ^2 - \phi_1(X,Y)) = \phi_2(X,Y)^2.$$

Every rational point of $\mathcal{D}$ can be lifted to a rational point on this pair of equations for some value of d. Also, the resultant of the 2 factors on the left hand side, together with the right hand side, of (2.1) is $2c$, and so the highest common factor is at most $2c$.

By considering $\mathcal{D}$ modulo 4, we see that we cannot have both X, Y odd (since then $X^4 + Y^4$ would be congruent to 2 (mod 4) and cZ^4 would be 0 mod 4), and we cannot have both X, Y even, since then Z would be even, contradicting the fact that the highest common factor of X, Y, Z is 1. So, Z is odd, exactly one of X, Y is odd, with the other even. Also, exactly one of a, b is odd and the other is even. Note also that

$$(a^2X^2 + b^2Y^2)(a^2Y^2 + b^2X^2) = c(X^2Y^2 + a^2b^2),$$

so that at least one of $a^2X^2 + b^2Y^2, a^2Y^2 + b^2X^2$ is divisible by c. For the following, we can exchange X and Y, if necessary, to guarantee that

$a^2X^2 + b^2Y^2$ is divisible by c, or we can exchange X and Y, if necessary, to guarantee that $a^2X^2 + b^2Y^2$ is odd, but we cannot necessarily do both of these simultaneously. We shall opt for swapping X and Y, if necessary, to guarantee that $a^2X^2 + b^2Y^2$ is divisible by c (which means that we shall have no control over whether it is also odd). We now have that each of the two factors on the left hand side of (2.1) is divisible by c. Since the highest common factor is at most $2c$, we have that the highest common factor is either $2c$ or c. This contrasts with the cover in [8] (p.187) and [20], where it was possible to guarantee the parity by (if necessary) swapping X and Y, and to guarantee c as a common factor by (if necessary) negating X or Y. This means that we shall end up with two genus 2 curves to consider, rather than 1.

For the case when the two factors on the left hand side of (2.1) have $2c$ as the highest common factor, we can write

$$cZ^2 + \phi_1 = 2cR^2, \tag{2.2}$$

$$cZ^2 - \phi_1 = 2cS^2, \tag{2.3}$$

$$\phi_2 = 2cRS, \tag{2.4}$$

for some R, S. We now want to rewrite these 3 equations as another set of 3 equations such that each is of the form **square** $= F(R, S)$, where F is some function in R and S. For this case, this is quite simple as, by using equations (2.2),(2.3),(2.4), we find that

$$(2.2) + (2.3) \Rightarrow Z^2 = (R^2 + S^2), \tag{2.5}$$

$$((2.2) - (2.3)) \times b^2 + ((2.4) \times 2a^2) \Rightarrow Y^2 = 2a^2RS + b^2(R^2 - S^2), \tag{2.6}$$

and

$$X^2 = a^2(R^2 - S^2) - 2b^2RS. \tag{2.7}$$

This means we have 3 quadratic equations in $\mathbb{P}^4$, a curve whose genus we do not require (it is stated on p.189 of [8] that the genus is 5; we do not require that fact here). Using the map $(R, S, X, Y, Z) \mapsto (R, S, T)$, where

$T = XYZ/S^2$, and using that the product of the left hand sides is equal to the product of the right hand sides, this curve covers a curve of genus 2,

$$T^2S^4 = (a^2(R^2 - S^2) - 2b^2RS)(2a^2RS + b^2(R^2 - S^2))(R^2 + S^2).$$

We can write this in affine form (taking $S = 1, R = x$ and $T = y$)

$$\mathcal{C} : y^2 = H_1(x)H_2(x)H_3(x), \tag{2.8}$$

with

$$H_1(x) = a^2x^2 - 2b^2x - a^2,$$

$$H_2(x) = b^2x^2 + 2a^2x - b^2,$$

$$H_3(x) = x^2 + 1.$$

In the case when the two factors on the left hand side of (2.1) have highest common factor c, we simply remove the factors of 2 on the right hand sides of each of (2.2),(2.3),(2.4). This has the effect of giving

$$\mathcal{C}' : y^2 = 2H_1(x)H_2(x)H_3(x). \tag{2.9}$$

In order to compute $\mathcal{D}(\mathbb{Q})$, when c is prime, it is therefore sufficient to compute $\mathcal{C}(\mathbb{Q})$ and $\mathcal{C}'(\mathbb{Q})$ for the above two curves $\mathcal{C}, \mathcal{C}'$ of genus 2.

2.2.3 Third cover

For the final cover, we write the general form of the curve $\mathcal{D}$ as

$$\{(cZ^2 + \psi_1(X,Y))(cZ^2 - \psi_1(X,Y)) = 2(\psi_2(X,Y))^2$$

with

$$\psi_1 = ((a^2 - b^2)X^2 + 2abXY + (b^2 - a^2)Y^2),$$

$$\psi_2 = (abX^2 + (b^2 - a^2)XY - abY^2).$$

Once again we continue in exactly the same way. After similar calculations, we get a similar situation to the previous part, where we have that the genus 2 curves relating to this cover are of the form

$$\mathcal{C}_d := y^2 = dJ_1(x)J_2(x),$$

where d is a factor of $2c$ and where:

$$\begin{aligned} J_1(x) &= x^2 + 2, \\ J_2(x) &= l_1x^4 + l_2x^3 + l_3x^2 + l_4x + l_5, \\ l_1 &= a^4 + 2a^2b^2 + b^4, \\ l_2 &= 8ab^3 - 8a^3b, \\ l_3 &= 12a^4 - 24a^2b^2 + 12b^4, \\ l_4 &= 16a^3b - 16ab^3, \\ l_5 &= 4a^4 + 8a^2b^2 + 4b^4. \end{aligned}$$

2.3 Examples using the covers

So, we have provided the general form for the covers which can be used to help resolve the Fermat Quartic for the family of values of c where c is prime of the form $c = a^4 + b^4$. However, we can in fact extend this c to any number of the form $c = a^4 + b^4$; that is, remove the condition of primality. We again get a set of genus 2 curves for each cover, which are all *twists* (that is, birationally equivalent over $\mathbb{C}$ but not over $\mathbb{Q}$). So geometrically they are the same curve. We illustrate this with the example $c = 82$, which can be written as $c = 1^4 + 3^4$ and is both the only value of $c \leq 100$ which is composite that requires using this genus 2 covering technique and the next on the list of unresolved cases ($c = 17$ and $c = 82$ are the first two values of c which cannot be resolved using either local arguments on $\mathcal{D}$ or a map to a rank 0 elliptic curve, and $c = 17$ was solved in [20]). We will illustrate the example $c = 82$ using the cover from [20]. Then we will also give examples of how to obtain the second cover (above) with the example $c = 17 = 1^2 + 2^2$.

Example 5. We look at the curve $\mathcal{D}_{82}$. Using notation from [20] we have the Jacobian of $\mathcal{D}_{82}$ reducible to $\mathcal{E}_1 \times \mathcal{E}_1 \times \mathcal{E}_2$. With the case of 82 we can perform

usual techniques to see that $\mathcal{E}_1$ has rank 3 and $\mathcal{E}_2$ has rank 2. Therefore we are unable to deduce immediately what the $\mathbb{Q}$-rational points on $\mathcal{D}_{82}$ are. Since [20] only discusses the case when c is prime, we need to work back through their cover to extend to the case $c = 82$.

The equation for the curve $\mathcal{D}_{82}$ can be written as

$$\{82Z^2 + (10X^2 - 6XY + 10Y^2)\}\{82Z^2 - (10X^2 - 6XY + 10Y^2)\}$$

$$= -2(3X^2 - 10XY + 3Y^2)^2. \tag{2.10}$$

Call this version $\widehat{\mathcal{D}}_{82}$. The two factors on the left-hand side of this do not have any common zeros on $\mathcal{D}_{82}$. Thus the double cover of $\mathcal{D}_{82}$ is given by the pair of equations

$$82Z^2 + (10X^2 - 6XY + 10Y^2) = dR^2,$$

$$dR^2\{82Z^2 - (10X^2 - 6XY + 10Y^2)\} = -2(3X^2 - 10XY + 3Y^2)^2.$$

Every rational point on $\mathcal{D}_{82}$ can be lifted to a rational point on this cover for some $d \in \mathbb{Z}$. The resultant of the two factors on the left hand side, together with the right hand side, of $\widehat{\mathcal{D}}_{82}$ is 328 and so there will be no rational solutions unless d divides 328. Let (X, Y, Z) be a rational point on $\mathcal{D}_{82}$. We may take X, Y, Z to be coprime integers. We can consider the equation $X^4 + Y^4 = 82Z^4$ reducing modulo 4. This tells us that the RHS is congruent to 0 if Z is even and congruent to 2 if Z is odd. The only way to have the LHS congruent to 0 mod 4 is for X, Y to be even, forcing Z also to be even, and this contradicts X, Y, Z being coprime. Therefore we deduce that Z must be odd. Also, since Z is odd, the only way to have the LHS congruent to 2 mod 4 is with X and Y both odd too. Therefore we have immediately that any $\mathbb{Q}$-rational points on $\mathcal{D}_{82}$ must have $X, Y, Z \not\equiv 0$ mod 2. Now let us consider the expression $(9X^2 - Y^2)(X^2 - 9Y^2)$; reducing this expression mod 82 (and using the fact that $X^4 + Y^4 = 82$), we get

$$(3X - Y)(X - 3Y)(3X + Y)(X + 3Y) = 9(X^4 + Y^4) - 82X^2Y^2 \equiv 0 \bmod 82$$

which means

$$(3X - Y)(X - 3Y)(3X + Y)(X + 3Y) \equiv 0 \bmod 2,$$

and

$$(3X - Y)(X - 3Y)(3X + Y)(X + 3Y) \equiv 0 \bmod 41.$$

This implies that

$$(3X - Y)(X - 3Y) \equiv 0 \bmod 41 \text{ or } (3X + Y)(X + 3Y) \equiv 0 \bmod 41.$$

Replacing Y with $-Y$, if necessary, we can assume that $(3X - Y)(X - 3Y) \equiv 0 \bmod 41$, and so the right hand side of (2.10) is divisible by 41. It follows from (2.10) that $10X^2 - 6XY + 10Y^2$ is also divisible by 41 and so each of the factors of the left hand side of (2.10) is divisible by 41.

Note that, since X and Y are odd, the right hand side of (2.10) is divisible by 8, so at least one of the factors on the left hand side is divisible by 4. Since these factors differ by a multiple of 4, both factors are divisible by 4. It follows that we can assume $d = 164$ or 328. We consider each case separately.

2.3.1 The case d=164

We have the equations

$$82Z^2 + (10X^2 - 6XY + 10Y^2) = 164R^2,$$

$$82Z^2 - (10X^2 - 6XY + 10Y^2) = -328S^2,$$

$$3X^2 - 10XY + 3Y^2 = 164RS,$$

for some integers R, S; that is

$$(X - Y)^2 = 28RS + 4R^2 + 8S^2,$$

$$(X + Y)^2 = 16R^2 - 52RS + 32S^2,$$

$$Z^2 = R^2 - 2S^2.$$

These equations cover the genus 2 curve

$$T^2S^4 = (16R^2 - 52RS + 32S^2)(4R^2 + 28RS + 8S^2)(R^2 - 2S^2).$$

We write this genus 2 curve in affine form

$$\mathcal{C}_1 : y^2 = (16x^2 - 52x + 32)(4x^2 + 28x + 8)(x^2 - 2).$$

2.3.2 The case d=328

We have the equations

$$82Z^2 + (10X^2 - 6XY + 10Y^2) = 328R^2,$$

$$82Z^2 - (10X^2 - 6XY + 10Y^2) = -656S^2,$$

$$3X^2 - 10XY + 3Y^2 = 328RS,$$

for some integers R, S; that is

$$(X - Y)^2 = 56RS + 8R^2 + 16S^2,$$

$$(X + Y)^2 = 32R^2 - 104RS + 64S^2,$$

$$Z^2 = 2R^2 - 4S^2.$$

These equations cover the genus 2 curve

$$T^2S^4 = (32R^2 - 104RS + 64S^2)(8R^2 + 56RS + 16S^2)(R^2 - 2S^2).$$

If we can show that the only rational points on this genus 2 curve (and those on the genus 2 curve $\mathcal{C}_1$ in the last section) are those with $S = 0$ then we could deduce that the only points on $\mathcal{D}_{82}$ are the obvious ones (over $\mathbb{Q}$ of course). We write this genus 2 curve in affine form

$$\mathcal{C}_2 : y^2 = (32x^2 - 104x + 64)(8x^2 + 56x + 16)(2x^2 - 4).$$

These curves relate to the method outlined in [20]. If we wanted to describe completely the rational points of this curve, we can not use Chabauty unfortunately because the rank of the Jacobian of each curve over the rationals is 2 and thus we would have to use the method in Flynn-Wetherell [20] completely (which works in the field $\mathbb{Q}(\sqrt{2}, \sqrt{c})$) to find, say, $\mathcal{C}_1(\mathbb{Q})$. However, the descent over this number field (for $c = 82$) was beyond the capabilities of packages such as Magma [40], and so it was not possible to resolve the case $c = 82$ in this way.

For our next example we will consider $c = 17, 82$, using the new covers.

Example 6. We consider the curve $\mathcal{D}_{17}$ so we can choose $c = a^4 + b^4 = 17 = 1^4 + 2^4$, so without loss of generality, $a = 1, b = 2$. Taking (2.8),(2.9), for the case when $a = 1, b = 2$ gives:

$$\mathcal{C} : y^2 = (x^2 - 8x - 1)(4x^2 + 2x - 4)(x^2 + 1).$$

$$\mathcal{C}' : y^2 = 2(x^2 - 8x - 1)(4x^2 + 2x - 4)(x^2 + 1).$$

We can now attempt to work out the rank of this curve. Using Magma [40] gives the rank of the Jacobian as 2, in each case, and so Chabauty's theorem is not applicable.

For the curve $\mathcal{D}_{82}$ we can use $a = 1, b = 3$ (since $82 = 1^4 + 3^4$) and then take (2.8),(2.9), for the case $a = 1, b = 3$, giving:

$$\mathcal{C} : y^2 = (x^2 - 18x - 1)(9x^2 + 2x - 9)(x^2 + 1).$$

$$\mathcal{C}' : y^2 = 2(x^2 - 18x - 1)(9x^2 + 2x - 9)(x^2 + 1).$$

Again, the rank of each $J(\mathbb{Q})$ is 2. Furthermore, if we attempt to imitate [20] by computing ranks over $\mathbb{Q}(\sqrt{2}, \sqrt{c})$ we find that Magma [40] is unable to perform the computation. Therefore our new covers do not currently resolve any new values of c, but they have the potential to do so later when computing power improves to the point where ranks over these number fields becomes possible.

2.4 Summary of how to attempt to find all rational points on $\mathcal{D}$

In the final section of this chapter, we will give a review of the methods that can be employed to find all the rational points on $\mathcal{D}$, and present them in an order that is logical. Also, we present a table of values of $c \leq 2000$ and identify the methods required (note: in the table, all values which can be resolved by local arguments are ignored).

1. **Local considerations.** If $\mathcal{D}$ is not locally solvable (in $\mathbb{R}$ or any $\mathbb{Q}_p$), then there can be no global solutions.

2. **The case when rank of $\mathcal{E}_1$ or $\mathcal{E}_2$ is 0.** If the rank of $\mathcal{E}_1$ or the rank of $\mathcal{E}_2$ is (unconditionally) 0, which can be verified by a computer package such as Apecs, then we have resolved $\mathcal{D}$. *Cases definitely resolved by this method are:* $c = 1, 2, 146, 226, 482, 562, 802$

3. $\mathcal{F}_1(\mathbb{Q}) = \phi$. Recall that $\mathcal{F}_1$ appears as a homogeneous space of $\mathcal{E}_1$ and has equation $X^2Z^2 + Y^4 = cZ^4$. Therefore we can class this as the most important homogeneous space as, if there are any points, they will occur on this space. If this is empty, then so is $\mathcal{D}(\mathbb{Q})$.

4. **If the rank of $\mathcal{E}_1$ is exactly 1 and the rank of $\mathcal{E}_2$ is non-zero**, In this case we *may* be forced to use the method of Manin-Dem'janenko. This method provides a bound on the height of a point as seen in [10]. However, in all the cases I have examined, whenever we have the opportunity to use this method, we have that $\mathcal{F}_1(\mathbb{Q}) = \phi$. The first example where this method was potentially applicable is $c = 2642$ (see above example). Of course one can still apply this method, but it is not necessary. (Note: these cases are extremely rare and there are only 2 such cases for $c \leq 5000$, namely $c = 2642$ and $c = 4226$).

5. $\mathcal{F}_1(\mathbb{Q}) \neq \phi$. Assuming that we have rational points on $\mathcal{F}_1$ and that the rank conditions above have not been met, we can attempt to use covers such as the 3 natural genus 2 covers described above. If the rank of any

of these $\mathcal{C}_i < 2$ then we can apply the theorem of Chabauty (Theorem 2, Section 2.1). Again, where computer technology can deal with the curves, this is extremely rare. We are unable to find an example with unconditional rank 1 for $c \leq 5000$, although $c = 257$ is the smallest c for which one of the $\mathcal{C}_i$ has odd Selmer bound (which by the parity conjecture lends itself to a lower bound of rank 1)

6. **If the rank of $\mathcal{C}_i \geq 2$.** In this case we can, in principle, imitate methods from [20] whereby we treat the genus 2 curve and consider a new elliptic curve over a number field. There are two types of new elliptic curve we can construct: the first is defined over a quadratic extension of $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt{2c})$. If this new elliptic curve has rank less than two then we can trace our way back to solve $\mathcal{D}(\mathbb{Q})$. The other alternative is a curve defined over a quartic extension of $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt{2}, \sqrt{c})$. If this elliptic curve has rank less than four then we can trace our way back to solve $\mathcal{D}(\mathbb{Q})$. However, it appears that number field packages are not yet capable of resolving new examples of this type, beyond the example computed in [20].

7. **Beyond these limits.** In all the cases I have considered, which computer algebra packages can cope with, all of the above methods resolve $\mathcal{D}$ for all its rational points.

Figure 2.1: Data for $c \leq 2000$

c	$a1$	$a2$	$a3$	$a4$	$a5$	$a6$
1	0	0	$(1,0)$			
2	1	0	$(1,1)$			
17	2	2	$(1,2)$			
82	3	2	$(1,3)$	4	8	4
97	2	2	$(2,3)$	4	4	
146	1	0				
226	3	0				
257	2	2	$(1,4)$	7	6	
337	2	2	$(3,4)$	7	6	
482	1	0				
562	1	0				
577	2	2				
626	3	2	$(1,5)$	4	8	
641	2	2	$(2,5)$	4	4	3
706	3	2	$(3,5)$			
802	1	0				
881	2	2	$(4,5)$	7		
977	2	0(2)				
1042	3	0(2)				
1186	1(3)	0(2)				
1201	2	0(2)				
1297	2	2	$(1,6)$			
1361	0(2)	0(2)				
1522	3	2				
1777	2	2				
1921	2	2	$(5,6)$			

The above table ignores all values of c which can be excluded by local considerations directly on $\mathcal{D}$. We again recall from Section 1 of [20], this means that any odd prime p dividing c must satisfy $p \equiv 1 \pmod 8$; furthermore $c \equiv 1, 2 \pmod{16}$, $c \not\equiv 3, 4 \pmod 5$, $c \not\equiv 7, 8, 11 \pmod{13}$, $c \not\equiv 4, 5, 6, 9, 13, 22, 28 \pmod{29}$.

In the above table the key is

c - value of c

$a1$ - 2-Selmer rank bound of $\mathcal{E}_1(\mathbb{Q})$

$a2$ - 2-Selmer rank bound of $\mathcal{E}_2(\mathbb{Q})$

$a3$ - point on the curve $\mathcal{D}$ in form (x, y)

$a4$ - (2-Selmer bound on the) rank of the Mordell-Weil group of the Jacobian of $\mathcal{C}_1$

$a5$ - (2-Selmer bound on the) rank of the Mordell-Weil group of the Jacobian of $\mathcal{C}_2$

$a6$ - (2-Selmer bound on the) rank of the Mordell-Weil group of the Jacobian of $\mathcal{C}_3$

Where $\mathcal{C}_1$ is the cover from [20], $\mathcal{C}_2$ is the first cover given above, while $\mathcal{C}_3$ is the remaining cover, with the quartic term.

Where for the elliptic curves there are 2 entries, this is because the first is the actual rank, whereas the number in brackets is the 2-Selmer bound for the rank (see the discussion immediately after Theorem 1) when processed using commands outlined in Appendix B using [40] or [38].

2.4.1 Generators

Here we provide a partial list of explicit generators corresponding to the ranks given in columns 1 and 2 of the table where the computations here relatively quick.

2a1 - (-1,1)
17a1 - (-1,4),(-4,2)
17a2 - (68,578),(144,1740)
82a1 - (-8,12),(18,66),(49/4,231/8)
82a2 - (2,116),(2624,134480)

97a1 - (-4,18),(49,336)

97a2 - (837/4,28227/8),(2903616/261121,43442841000/133432831)

146a1 - (81/4,585/8)

226a1 - (18,42),(-128/9,496/27),(121/4,1155/8)

257a1 - (-16,4),(169/9,1144/27)

257a2 - (4112,264196),($\frac{808618189824}{2709098401}$, $\frac{959532007033871520}{141005862673649}$)

As can be seen, with generators this size, it would have been very difficult to even attempt to complete the table or find generators for any of the Jacobians of the genus 2 curves considered.

Chapter 3

The Bielliptic Isogeny

In this chapter we will outline the ideas behind a bielliptic isogeny.

Definition 8. A curve of genus 2 is called *bielliptic* if it has a degree 2 map to an elliptic curve.

As in Section 2 of [17], we shall concentrate on curves of genus 2

$$\mathcal{C} : Y^2 = F(X) = f_6X^6 + \ldots + f_0, \tag{3.1}$$

defined over a number field K, for which there exists an involution $\tau(X) = (aX + b)/(cX + d)$, defined over K, which permutes the roots of $F(X)$; let us say that τ swaps the six roots of $F(X)$ according to: $\alpha_1 \leftrightarrow \alpha_1'$, $\alpha_2 \leftrightarrow \alpha_2'$, $\alpha_3 \leftrightarrow \alpha_3'$. We recall from Section 2 of [17] that the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ associated to τ must have its square equal to $\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$, for some $k \in K$, and so has eigenvalues $\pm\sqrt{k}$, with corresponding eigenvectors $(s_1\ t_1), (s_2\ t_2)$. Furthermore, $\sigma(X) = (s_1X + t_1)/(s_2X + t_2)$ is negated by $X \mapsto \tau(X)$, and $\sigma(X)^2$ is invariant, so that there exist cubics G^a, G^b defined over $K(\sqrt{k})$ such that $\phi^a : (X, Y) \mapsto (\sigma(X)^2, Y/(s_2X+t_2)^3)$ and $\phi^b : (X, Y) \mapsto (1/\sigma(X)^2, Y/(s_1X+t_1)^3)$ map $\mathcal{C}$ to

$$\begin{aligned} \mathcal{E}^a &: y^2 = G^a(x) = g_3^a x^3 + g_2^a x^2 + g_1^a x + g_0^a, \\ \mathcal{E}^b &: y^2 = G^b(x) = g_3^b x^3 + g_2^b x^2 + g_1^b x + g_0^b, \end{aligned} \tag{3.2}$$

respectively. Hence any such $\mathcal{C}$ is bielliptic. Let $A = \mathcal{E}^a \times \mathcal{E}^b$. As in Theorem 4.2 of [33], these induce the isogeny $\phi = (\phi^a)^* + (\phi^b)^* : A \to J$, and the dual isogeny $\hat{\phi} = (\phi^a)_* \times (\phi^b)_* : J \to A$. The compositions $\phi' \circ \phi$ and $\phi \circ \phi'$ are the multiplication by 2 maps on A and J, respectively. Recall from [29] (Remark 3.4 of Chapter II) that, for any map $\phi : \mathcal{C}_1 \to \mathcal{C}_2$ between any two smooth curves $\mathcal{C}_1, \mathcal{C}_2$, ϕ^* is the map from $\mathrm{Pic}^0(\mathcal{C}_2)$ to $\mathrm{Pic}^0(\mathcal{C}_1)$ which takes $[Q]$ to $\sum_{P \in \phi^{-1}(Q)} e_\phi(P)[P]$, and ϕ_* is the map from $\mathrm{Pic}^0(\mathcal{C}_1)$ to $\mathrm{Pic}^0(\mathcal{C}_2)$ which takes $[P]$ to $[\phi(P)]$ [the notation $e_\phi(P)$ denotes the ramification index of ϕ at P, which is defined at the top of p.11 of [29]]. Note that we merely use the explicit forms of ϕ and $\hat{\phi}$, which are already derived in Theorem 4.2 of [33].

Note that the map $(X, Y) \mapsto (\sigma(X), Y/(s_2X + t_2)^3)$ is a birational equivalence over $\bar{K}$ to the curve

$$\mathcal{C}' : Y^2 = G^a(X^2).$$

We summarise as follows.

Theorem 3. *Suppose $\mathcal{C} : Y^2 = f_6X^6 + \ldots + f_0$ is a genus 2 curve defined over a number field K, for which there exists an involution $\tau(X) = (aX + b)/(cX + d)$, defined over K, which permutes the roots of $F(X)$. Then the Jacobian of $\mathcal{C}$ is isogenous over K to $A = \mathcal{E}^a \times \mathcal{E}^b$ of (3.2). The curve $\mathcal{C}$ is birationally equivalent over $\bar{K}$ to a curve of the form $C' : Y^2 = G^a(X^2)$, where G^a is cubic. Furthermore:*

1. *$\mathcal{C}$ has degree 2 maps to two genus 1 curves $\mathcal{E}^a$ and $\mathcal{E}^b$.*
2. *There is a polynomial $r(x) \in \bar{K}[x]$ such that $\mathcal{C}'$, $\mathcal{E}^a$, and $\mathcal{E}^b$ have equations of the form*

$$\begin{array}{rrcccl} \mathcal{C}' : & Y^2 & = & r(X^2) & = & r_3X^6 + r_2X^4 + r_1X^2 + r_0. \\ \mathcal{E}^a : & y^2 & = & r(x) & = & r_3x^3 + r_2x^2 + r_1x + r_0. \\ \mathcal{E}^b : & y^2 & = & x^3 \cdot r(x^{-1}) & = & r_0x^3 + r_1x^2 + r_2x + r_3. \end{array}$$

There are degree 2 maps $\phi'_a : \mathcal{C}' \to \mathcal{E}^a$ and $\phi'_b : \mathcal{C}' \to \mathcal{E}^b$ given by $\phi'_a(x, y) = (x^2, y)$ and $\phi'_b(x, y) = (1/x^2, y/x^3)$.

3.1 The maps ϕ_a and ϕ_b

Given a curve $\mathcal{C}$ as in Theorem 3, we can write the birationally equivalent curve over $\bar{K}$ as

$$\mathcal{C}' : Y^2 = k(X^2 - e_1)(X^2 - e_2)(X^2 - e_3). \tag{3.3}$$

We have the map $\phi'_a : \mathcal{C}' \to \mathcal{E}^a$ given by $\phi'_a(X, Y) = (X^2, Y)$ and the map $\phi'_b : \mathcal{C}' \to \mathcal{E}^b$ given by $\phi'_b(X, Y) = (1/X^2, Y/X^3)$. So $\mathcal{E}^a : Y^2 = k(X - e_1)(X - e_2)(X - e_3)$ and $\mathcal{E}^b : W^2 = k(1 - e_1V)(1 - e_2V)(1 - e_3V)$ are typical forms of these curves. Then, $\phi' = (\phi'_a)^* + (\phi'_b)^*$ from $A \to J'$ (where J' is the Jacobian of $\mathcal{C}'$), and $\hat{\phi}' = (\phi'_a)_* \times (\phi'_b)_*$ from $J' \to A$, are, respectively, an isogeny and its dual isogeny and we can write ϕ' and $\hat{\phi}'$ explicitly in this case as,

$$\begin{aligned} \phi([(X, Y), (V, W)]) &= \{(\sqrt{X}, Y), (-\sqrt{X}, Y)\} \\ &\quad \oplus \{(1/\sqrt{V}, W/V\sqrt{V}), (-1/\sqrt{V}, -W/V\sqrt{V})\} \end{aligned}$$

where $\oplus$ denotes addition on $J(\mathbb{Q})$.

$$\hat{\phi}(\{(X_1, Y_1), (X_2, Y_2)\}) = [(X_1^2, Y_1) +_a (X_2^2, Y_2), \left(\frac{1}{X_1^2}, \frac{Y_1}{X_1^3}\right) +_b \left(\frac{1}{X_2^2}, \frac{Y_2}{X_2^3}\right)]$$

where $+_a$ denotes addition on $\mathcal{E}^a$ and $+_b$ denotes addition on $\mathcal{E}^b$.

Lemma 2. *Given $\mathcal{C}'$ as in (3.3), we can describe completely the kernel of both ϕ' and $\hat{\phi}'$ as*

$$\begin{aligned} \ker \phi' &= \{id_A\} \cup \{[(e_i, 0), (1/e_i, 0)] : i = 1, 2, 3\}, \\ \ker \hat{\phi}' &= \{id_{J'}\} \cup \{\{(\sqrt{e_i}, 0), (1/\sqrt{e_i}, 0)\} : i = 1, 2, 3\}. \end{aligned}$$

Proof. For ϕ' we are looking for elements which map to the identity in J'. It is easy to see that $\phi'(\{id_A, [(e_i, 0), (1/e_i, 0)]\}) = id_{J'}$. To show that this is all members of the kernel, consider what the element $id_{J'}$ looks like. It will be of the form $\{(r, s), (r, -s)\}$. If we consider our addition on J', from the definition of ϕ', to ensure the result of the addition is of the required form,

then we have the equations $\sqrt{X} = \frac{1}{\sqrt{V}}$, $Y = \frac{W}{V\sqrt{V}}$ and $Y = \frac{-W}{V\sqrt{V}}$. The 2^{nd} and 3^{rd} of these, when added together, give $Y = 0$, so $W = 0$. Into the equations for $\mathcal{E}^a$ and $\mathcal{E}^b$ gives $X = e_1, e_2, e_3$, and $v = 1/e_1, 1/e_2, 1/e_3$. In order to satisfy the equation $\sqrt{X} = \frac{1}{\sqrt{V}}$, we see that the elements claimed in to be in the kernel are all such elements. A similar argument shows ker $\hat{\phi}'$ is as claimed. ∎

Note that, given any curve of the form $\mathcal{C} : Y^2 = f_6X^6 + \ldots + f_0$ with an involution $\tau(X)$ on the roots of the sextic, the above allows us to describe the kernels of ϕ and $\hat{\phi}$ by composing the above kernels with the map between J and J' induced by the birational transformation between $\mathcal{C}$ and $\mathcal{C}'$.

We can also see directly the effect of composing the isogenies.

Lemma 3. *Given $\mathcal{C}'$ as in (3.3). Both $\phi' \circ \hat{\phi}'$ and $\hat{\phi}' \circ \phi'$ are the multiplication by 2 map.*

Proof. We have

$$\begin{aligned}
&\hat{\phi}'(\phi'([(X,Y),(V,W)])) \\
&= \hat{\phi}'(\{(\sqrt{X},Y),(-\sqrt{X},Y)\} \\
&+\{(1/\sqrt{V},W/V\sqrt{V}),(-1/\sqrt{V},-W/V\sqrt{V})\}) \\
&= \hat{\phi}'\{(\sqrt{X},Y),(-\sqrt{X},Y)\} \\
&+\hat{\phi}'\{(1/\sqrt{V},W/V\sqrt{V}),(-1/\sqrt{V},-W/V\sqrt{V})\} \\
&= [(X,Y)+(X,Y),(1/X,Y/X\sqrt{X})+(1/X,-Y/X\sqrt{X})] \\
&+[(1/V,W/V\sqrt{V})+(1/V,-W/V\sqrt{V}),(V,W)+(V,W)] \\
&= [2(X,Y),\infty]+[\infty,2(V,W)] \\
&= [2(X,Y),2(V,W)] \\
&= 2[(X,Y),(V,W)].
\end{aligned}$$

So indeed we have $\hat{\phi}' \circ \phi' =$ multiplication by 2. Similarly for $\phi' \circ \hat{\phi}'$. ∎

Note again that, in our original case, for any curve of the form $\mathcal{C} : Y^2 = f_6X^6 + \ldots + f_0$ with an involution $\tau(X)$ on the roots of the sextic, $\hat{\phi} \circ \phi$

and $\phi \circ \hat{\phi}$ are given by multiplication by 2, since $\mathcal{C}$ and $\mathcal{C}'$ are birationally equivalent (so that J and J' are isomorphic).

3.2 The q map in a special case

In this section we will consider the map called μ in Equation (7) of [17], which we call q. We will use this map in conjunction with curves of genus 2, which are bielliptic and of the form $\mathcal{C} : y^2 = F_0(X)F_1(X)F_2(X)$ with F_i at most quadratic in degree, with F_0 defined over K and F_1, F_2 defined over either K or some quadratic extension such as $K(\sqrt{d})$, and where $F_0 = \lambda_1 F_1 + \lambda_2 F_2$, for some λ_1, λ_2 members of the field of definition of F_1, F_2. In this latter case of course F_1, F_2 are conjugate over this quadratic extension to ensure $\mathcal{C}$ is defined over K. Note that the $\tau(X) = (aX + b)/(cX + d)$ which swaps the roots of F_1 and swaps the roots of F_2, will also swap the roots of F_0 (see Theorem 14.1.1 of [8]) and so the curve is bielliptic, and we can refer to $A = \mathcal{E}^a \times \mathcal{E}^b$ and $\phi : A \to J$, as in the previous sections. Using Equation (7) of [17] in this case (and renaming μ as q) gives:

$$\begin{aligned} q = [q_1, q_2, q_3] \quad &: \quad J(K)/\phi(A(K)) \to \\ &\quad K^*/(K^*)^2 \times K(\sqrt{d})^*/(K(\sqrt{d})^*)^2 \times K(\sqrt{d})^*/(K(\sqrt{d})^*)^2 \\ &: \quad \{(X_1, Y_1), (X_2, Y_2)\} \to \\ &\quad [F_0(X_1)F_0(X_2), F_1(X_1)F_1(X_2), F_2(X_1)F_2(X_2)]. \end{aligned} \tag{3.4}$$

The following is from [28] (Lemma 2.1 and Proposition 2.2).

Lemma 4. *The above map q is an injective homomorphism of groups.*

There is an associated map q' which is referred in [17] as μ'. This map of course has similar properties to q, but is instead on $A(K)/\hat{\phi}(J(K))$; we shall not need to make any use of the map q'.

Chapter 4

Bielliptic curves of genus two

In this chapter we will consider bielliptic curves of genus two. We will be concerned with looking at bielliptic curves as considered in [17]. Flynn and Redmond look for $\mathbb{Q}$-rational points on a number of examples, using a method which is described as being "up-down". They start with a genus two curve, where the usual methods are unable to determine all the points, and use covering to go "up" to a genus five covering curve, then "down" to elliptic curves and back up to a new genus two curve, which they hope will be more compliant when applying techniques such as Chabauty etc. In this chapter we will be concerned with describing their method in a more fluid way, working it through in a general setting whereas they consider solely certain families of curves. There are several subtleties required in this general context, not immediately apparent from the example in [17].

Next we will examine the suggestion from [17] that the method will cycle after a finite number of applications - we show this to be true using their example. We used the computer package Maple to deal with some of the algebra involved, details of which are found at my website in the file "progs.txt" at *http://www.liv.ac.uk/~mp0u8024/maths/* and in Appendix B. Finally we provide a counterexample to computing all of the rational points on a curve of genus 2 using this method.

4.1 Relevance of the method to help find all the K-rational points

We first give some context and motivation. We shall consider curves of genus 2, defined over a number field K, of the form

$$\mathcal{C} \ : \ y^2 \ = \ F_0F_1F_2, \tag{4.1}$$

where

$$F_1 = a_1X^2 + b_1X + c_1, \ F_2 = a_2X^2 + b_2X + c_2, \ F_0 = k_1F_1 + k_2F_2, \tag{4.2}$$

with $a_1, a_2 \neq 0$ and such that $F_0F_1F_2$ has no repeated zeroes. We suppose moreover that F_1, F_2 are either both defined over K or are defined over a quadratic extension $K(\sqrt{d})$ of K and are conjugate over K, and that F_0 is a linear combination of F_1 and F_2 defined over K and is non-constant (we allow the possibility that F_0 is linear). In order to consider these two cases together, we allow $d = 1$ to cover the case where F_1 and F_2 are defined over K, but must remember that in this case F_1 and F_2 are not conjugate. If we know at least one $P_0 \in \mathcal{C}(K)$, say that P_0 is a point at infinity, and that we have computed $J(K)/\phi(A(K)) = \{D_1, \ldots, D_m\}$. Following Equation (9) of [17], let $\mathcal{C}_i$ be the image of $\mathcal{C}$ in J via $f_i : P \mapsto [P - P_0] - D_i$, let $\mathcal{D}_i$ be the pullback of $\mathcal{C}_i$ to A via ϕ, and J_i be the Jacobian of $\mathcal{D}_i$, in which case J_i is isogenous to the product of the Jacobian of $\mathcal{C}$ and the Jacobians of the following three curves of genus 1, defined over $K, K(\sqrt{d}), K(\sqrt{d})$, respectively (a special case of (9) of [17]):

$$\mathcal{E}_{i,j} : y_{i,j}^2 = q_j(D_i)F(X)/F_j(X), \ j = 0, 1, 2, \tag{4.3}$$

where q_0, q_1, q_2 are as in (3.4). In order to find all of $\mathcal{C}(K)$ it is sufficient, for each i, to find all of $\mathcal{E}_{i,0}(K)$ or to find all $(X, Y) \in \mathcal{E}_{i,1}(K(\sqrt{d}))$ with $X \in K$, or to find all $(X, Y) \in \mathcal{E}_{i,2}(K(\sqrt{d}))$ with $X \in K$. When $d \neq 1$, the last two of these are equivalent, since $\mathcal{E}_{i,1}, \mathcal{E}_{i,2}$ are quadratic and conjugate over K. We shall see that there is a 2-to-1 map (defined over K when $j = 0$ and defined

over $K(\sqrt{d})$ otherwise) from each genus 1 curve $\mathcal{E}_{i,j}$ to an elliptic curve $\mathcal{E}'_{i,j}$ (of the standard form **square** = cubic in x), where there is a K-rational map which gives the x-coordinate of each $\mathcal{E}'$ in terms of the X-coordinate of $\mathcal{E}$. So now, in order to find all of $\mathcal{C}(K)$ it is sufficient, for each i, to find all of $\mathcal{E}'_{i,0}(K)$ or to find all $(x,y) \in \mathcal{E}'_{i,1}(K(\sqrt{d}))$ with $x \in K$, or to find all $(x,y) \in \mathcal{E}'_{i,2}(K(\sqrt{d}))$ with $x \in K$ (again, the last two of these are equivalent, since $\mathcal{E}'_{i,1}, \mathcal{E}'_{i,2}$ are quadratic and conjugate over K).

Now, finding all of $\mathcal{E}'_{i,0}(K)$ is possible only when the rank of $\mathcal{E}'_{i,0}(K)$ is 0. We shall see that we can find a new bielliptic curve $\mathcal{C}_i$ of genus 2, defined over K, with maps from $\mathcal{C}_i$ to $\mathcal{E}'_{i,1}$ and $\mathcal{E}'_{i,2}$ which are K-rational on the X-coordinates, such that any $(x,y) \in \mathcal{E}'_{i,1}(K(\sqrt{d}))$ with $x \in K$, gives rise to $(X,Y) \in \mathcal{C}_i(K)$. In summary, in order to find $\mathcal{C}(K)$, it is sufficient, for each $i = 1, \ldots, n$, either to find $\mathcal{E}'_{i,0}(K)$ or to find $\mathcal{C}_i(K)$. This gives rise to the following method for trying to find $\mathcal{C}(K)$.

Method 1. Let $\mathcal{C}$ be as in (4.1) and suppose further that the coefficient of X^6 in $\mathcal{C}$ is a square in K (so that ∞^+, ∞^- belong to $\mathcal{C}(K)$). Let the elliptic curves $\mathcal{E}'_{i,0}$ and genus 2 curves $\mathcal{C}_i$ be as described above, with Jacobian J_i, for $i = 1, \ldots, m$. Suppose that, for each i, either the 2-Selmer bound on the rank of $\mathcal{E}'_{i,0}(K)$ is 0 or the 2-Selmer bound on the rank of $J_i(K)$ is less than 2. In the first case, we can find all of $\mathcal{E}'_{i,0}(K)$; in the second case, we can apply Chabauty's Theorem (Theorem 2, Section 2.1) and hope that this give us all of $\mathcal{C}_i(K)$.

This is referred to in [17] as an "up-down" method, as we are going up and down via 2-to-1 maps between curves. There are several places where this method could potentially fail; in particular, it is guaranteed to fail if there exists an i for which the rank of $\mathcal{E}'_{i,0}(K)$ is > 0 and the rank of $J_i(K)$ is > 1. In [17] it is shown that there are infinitely many curves for which one application of this method fails, by investigating curves of the form $Y^2 = (X^2 + p)(X^4 + p^2)$. The computations in [17] were somewhat atypical, as the involution is $X \mapsto -X$ which does not indicate completely how to handle the more general case. For the rest of the chapter, we shall give the details of how to construct these curves for any starting curve of the form $Y^2 = F_0F_1F_2$, satisfying the conditions of Method 1. Since we will finally

be aiming at a counterexample, we shall consider only the case when D_i is the identity element. The benefit of the rest of this chapter is that we shall derive equations for the various steps in this more general context (which was not done in [17], where the curve $Y^2 = (X^2 + p)(X^4 + p^2)$ was handled ad hoc). This series of equations will give an easier way for anyone to apply the method to any curve of this type. Furthermore, there is the possibility of repeated applications of the method, since the final curves C_i are of genus 2 and are bielliptic. In the next chapter, we shall follow through repeated applications of the method, for the case when D_i is the identity element, to the curves $Y^2 = (X^2+p)(X^4+p^2)$, and show that there is eventual cycling. Furthermore we shall show that, for some values of p, the method fails, however many times it is repeatedly applied.

4.2 The details of the "up-down" method

Let $\mathcal{C}$ be a curve as in (4.1). There exists an involution on $\mathbb{P}^1$ which swaps the roots of each of F_1 and F_2 (and therefore F_0 since this is a linear combination of F_1 and F_2). This involution, which we call τ, can be explicitly described in terms of the coefficients of F_1 and F_2.

Lemma 5. *The involution τ which swaps the roots of each F_i is given by the formula*

$$\tau(X) = \frac{(a_1c_2 - a_2c_1)X + (b_1c_2 - c_1b_2)}{(a_2b_1 - a_1b_2)X + (a_2c_1 - a_1c_2)}.$$

Proof. There is a unique involution which swaps two pairs of numbers, say r_1, r_2 with s_1, s_2. If we set $t(X) = \frac{aX+b}{cX+d}$, then to ensure we have t which swaps the numbers, we will get 4 equations to solve for $\{a, b, c, d\}$. The equations are

$$\frac{ar_1 + b}{cr_1 + d} = s_1,$$

$$\frac{as_1 + b}{cs_1 + d} = r_1,$$

$$\frac{ar_2 + b}{cr_2 + d} = s_2,$$

$$\frac{as_2 + b}{cs_2 + d} = r_2.$$

Solving these equations for a, b, c, d gives:

$$a = r_1 s_1 - r_2 s_2,$$

$$b = (r_1 + s_1) r_2 s_2 - r_1 s_1 (r_2 + s_2),$$

$$c = (r_1 + s_1) - (r_2 + s_2),$$

$$d = r_2 s_2 - r_1 s_1.$$

If r_1, s_1 are the roots of F_1 and r_2, s_2 the roots of F_2, then

$$a_1 X^2 + b_1 X + c_1 = a_1 (X - r_1)(X - s_1)$$

and

$$a_2 X^2 + b_2 X + c_2 = a_2 (X - r_2)(X - s_2)$$

so that

$$r_1 + s_1 = \frac{-b_1}{a_1},$$

$$r_1 s_1 = \frac{c_1}{a_1},$$

$$r_2 + s_2 = \frac{-b_2}{a_2},$$

$$r_2 s_2 = \frac{c_2}{a_2},$$

which on substitution gives the required $t = \tau$. Since F_0 is a linear combination of F_1, F_2, this same τ also swaps the roots of F_0. ∎

Since $F_0 = k_1 F_1 + k_2 F_2$, we can work out k_1, k_2 in terms of the F_i, as

$$k_1 = \frac{b_2 a_0 - b_0 a_2}{a_1 b_2 - a_2 b_1}; \quad k_2 = \frac{a_1 b_0 - b_1 a_0}{a_1 b_2 - a_2 b_1}.$$

$$k_1 = \frac{c_2 a_0 - c_0 a_2}{a_1 c_2 - a_2 c_1}; \quad k_2 = \frac{a_1 c_0 - c_1 a_0}{a_1 c_2 - a_2 c_1}.$$

$$k_1 = \frac{b_2c_0 - b_0c_2}{c_1b_2 - c_2b_1}; \quad k_2 = \frac{c_1b_0 - b_1c_0}{c_1b_2 - c_2b_1}.$$

depending on which of the denominators is non-zero.

Now that we have the involution, we wish to find the function $\sigma(X)$ which will be negated by τ, so that $\sigma(X)^2$ is invariant. In [17] this $\sigma(X)$ is defined in terms of eigenvalues of the matrix associated to τ. It is in fact more convenient to write it explicitly in terms of the coefficients of the F_i and some resultants. First note that the eigenvalues of the matrix

$$\begin{pmatrix} a_1c_2 - a_2c_1 & b_1c_2 - c_1b_2 \\ a_2b_1 - a_1b_2 & a_2c_1 - a_1c_2 \end{pmatrix} \tag{4.4}$$

associated with τ, are $\pm\sqrt{R}$, where R is the resultant of F_1, F_2 with respect to X. Provided $a_1b_2 - b_1a_2 \neq 0$, we can take as corresponding nonzero eigenvectors:

$$[1, (a_1c_2 - a_2c_1 - \sqrt{R})/(a_1b_2 - b_1a_2)],$$

$$[1, (a_1c_2 - a_2c_1 + \sqrt{R})/(a_1b_2 - b_1a_2)],$$

which we might as well multiply through by the scalar $a_1b_2 - b_1a_2$ to give:

$$[a_1b_2 - a_2b_1, a_1c_2 - a_2c_1 - \sqrt{R}],$$

$$[a_1b_2 - a_2b_1, a_1c_2 - a_2c_1 + \sqrt{R}],$$

where we are taking our vectors to be row vectors, and multiplying with the row vector on the left, and the 2×2 matrix on the right.

When $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 \neq 0$ we can instead take as our nonzero eigenvectors:

$$[a_1c_2 - c_1a_2 + \sqrt{R}, b_1c_2 - b_2c_1],$$

$$[a_1c_2 - c_1a_2 - \sqrt{R}, b_1c_2 - b_2c_1].$$

When both expressions are zero, then we can take $[1, 0], [0, 1]$ as our eigenvectors.

Given eigenvectors $[s_1, s_2], [t_1, t_2]$ of the above matrix (4.4) corresponding to τ, for the eigenvalues $\sqrt{R}, -\sqrt{R}$, respectively, we have the following identity of matrices.

$$\begin{pmatrix} s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \begin{pmatrix} a_1c_2 - a_2c_1 & b_1c_2 - c_1b_2 \\ a_2b_1 - a_1b_2 & a_2c_1 - a_1c_2 \end{pmatrix} = \sqrt{R} \begin{pmatrix} s_1 & s_2 \\ -t_1 & -t_2 \end{pmatrix}.$$

Since composition of fractional linear transformations gives the same result as matrix multiplication of the corresponding matrices, it follows that $\sigma(X) = (s_1X + s_2)/(t_1X + t_2)$ is negated by replacing X with $\tau(X)$. We summarise this in the following lemma.

Lemma 6. *Let C be as in (4.1) and τ as in Lemma 5 and let us introduce $R = resultant(F_1, F_2, X)$, then there exists a function $\sigma(X)$, which is negated by τ [that is, $\sigma(\tau(X)) = -\sigma(X)$] so that its square is invariant under τ. This $\sigma(X)$ can be explicitly described as one of the following 3 cases.*
Case 1: $a_1b_2 - b_1a_2 \neq 0$

$$\sigma(X) = \frac{(a_1b_2 - b_1a_2)X + a_1c_2 - a_2c_1 - \sqrt{R}}{(a_1b_2 - b_1a_2)X + a_1c_2 - a_2c_1 + \sqrt{R}}.$$

Case 2: $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 \neq 0$

$$\sigma(X) = \frac{(a_1c_2 - c_1a_2 + \sqrt{R})X + b_1c_2 - b_2c_1}{(a_1c_2 - c_1a_2 - \sqrt{R})X + b_1c_2 - b_2c_1}.$$

Case 3: $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 = 0$

$$\sigma(X) = X.$$

Proof. This was already established in the discussion preceding the statement of the lemma; alternatively, one can simply check directly, in each case, that $\sigma(\tau(X)) = -\sigma(X)$, which leads to $\sigma(X)^2$ being invariant under τ. Notice that the first case is the most general, the second case imposes a condition and the final case is the most specialised (with 2 conditions). For all of the cases, we can verify that indeed $\sigma(X)$ is negated by τ simply by substitution.

∎

Lemma 7. *Let $\sigma(X)$ and R be as in Lemma 6. Then $\sigma(X)$ is defined over the number field $K(\sqrt{dR})$, where d is such that F_1 and F_2 are defined over $K(\sqrt{d})$.*

Proof. When $d = 1$ this is clear. Otherwise $\sigma(X)$ is defined over the quartic number field $K(\sqrt{d}, \sqrt{R})$. Note that the combined action $\sqrt{d} \to -\sqrt{d}$, $\sqrt{R} \to -\sqrt{R}$, swaps F_1 and F_2, negates the numerator and denominator of $\sigma(X)$ and so leaves it unchanged. Therefore we have immediately that $\sigma(X)$ is indeed defined over $K(\sqrt{dR})$. ∎

Now, we let T denote $\sigma(X)$ and we can invert $\sigma(X)$, which gives:

$$T = \sigma(X) \iff X = \sigma^{-1}(T) = \frac{-((a_1c_2 - a_2c_1)(T-1) + \sqrt{R}(T+1))}{(a_1b_2 - a_2b_1)(T-1)}. \tag{4.5}$$

If we replace X by $\sigma^{-1}(T)$ in the equation of $\mathcal{C}$ and multiply both sides by $R(a_1b_2 - a_2b_1)^6(T-1)^6$, our curve $\mathcal{C}$ becomes:

$$\left(Y\sqrt{R}(a_1b_2 - a_2b_1)^3(T-1)^3\right)^2 = RF_{0x}(T^2)F_{1x}(T^2)F_{2x}(T^2),$$

where

$$\begin{aligned} F_{1x}(x) &= 2a_1R(x+1) + (-2a_1a_2c_1 + 2a_1^2c_2 + a_2b_1^2 - b_1a_1b_2)\sqrt{R}(x-1), \\ F_{2x}(x) &= 2a_2R(x+1) + (-2a_2^2c_1 + 2a_2a_1c_2 - a_1b_2^2 + b_2a_2b_1)\sqrt{R}(x-1), \\ F_{0x}(x) &= k_1F_{1x}(x) + k_2F_{2x}(x). \end{aligned} \tag{4.6}$$

In summary (see Theorem 3),

$$(X, Y) \mapsto (T, y) = (\sigma(X), Y\sqrt{R}(a_1b_2 - a_2b_1)^3(\sigma(X) - 1)^3)$$

gives a birational trasformation between $\mathcal{C}$ and the curve

$$y^2 = RF_{0x}(T^2)F_{1x}(T^2)F_{2x}(T^2),$$

so that the map

$$\phi^a : (X, Y) \mapsto (x, y) = (\sigma(X)^2, Y\sqrt{R}(a_1b_2 - a_2b_1)^3(\sigma(X) - 1)^3) \qquad (4.7)$$

gives a map from $\mathcal{C}$ to the elliptic curve

$$\mathcal{E}^a : y^2 = RF_{0x}(x)F_{1x}(x)F_{2x}(x). \qquad (4.8)$$

Similarly the map $\phi^b : (X, Y) \mapsto (\underline{x}, \underline{y}) = (1/\sigma(X)^2, y/\sigma(X)^3)$, where y is as in (4.7), maps $\mathcal{C}$ to

$$\mathcal{E}^b : \underline{y}^2 = R\underline{x}^3F_{0x}(1/\underline{x})F_{1x}(1/\underline{x})F_{2x}(1/\underline{x}). \qquad (4.9)$$

Letting $A = \mathcal{E}^a \times \mathcal{E}^b$, we have $\phi = (\phi^a)^* + (\phi^b)^* : A \to J$, where J is the Jacobian of $\mathcal{C}$. Note that, if $d \neq 1$, $\mathcal{E}^a$ and $\mathcal{E}^b$ are quadratic and conjugate over K, and so A is defined over K, as is the map ϕ.

The above applies when $a_1b_2 - b_1a_2 \neq 0$. In the case when $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 \neq 0$, everything is as above, except that we start with the formula for σ, as in the second case of Lemma 6. In the case when $a_1b_2 - b_1a_2 = 0$ and $b_1c_2 - c_1b_2 = 0$, then $b_1 = b_2 = 0$ (otherwise there would be repeated roots in the right hand side of $\mathcal{C}$, contradicting the fact that $\mathcal{C}$ is of genus 2), and so we already have that $\mathcal{C}$ is of the form $Y^2 = G(X^2) = r_3X^6 + r_2X^4 + r_1X^2 + r_0$; in this case, we have our simplified situation that the maps $(X, Y) \mapsto (x, y) = (X^2, Y)$ and $(X, Y) \mapsto (\underline{x}, \underline{y}) = (1/X^2, Y/X^3)$ are, respectively, from $\mathcal{C}$ to $\mathcal{E}^a : r_3X^3 + r_2X^2 + r_1X + r_0$ and $\mathcal{E}^b : r_0X^3 + r_1X^2 + r_2X + r_3$.

4.2.1 Focusing on the identity case

We have in [17] (and as summarised at the beginning of this chapter) that, through the covering technique described there, the problem of finding $\mathcal{C}(K)$ is reduced to finding, for each i, all $(X, Y) \in \mathcal{E}_{i,j}$ with $X \in K$ for at least

one of $j = 0, 1, 2$, where

$$\mathcal{E}_{i,j} : y_{i,j}^2 = q_j(D_i)F(X)/F_j(X), j = 0, 1, 2,$$

with q as described in Chapter 3 and $D_i \in J(K)/\phi(A(K))$. We will not be so interested in finding all of $\mathcal{C}(K)$.

We will focus on the case when

$$D_i = id$$

so that

$$q_j(D_i) = 1.$$

Thus our three genus 1 curves will be

$$\begin{aligned} \mathcal{E}_0 &: Y_0^2 = F_1(X)F_2(X), \\ \mathcal{E}_1 &: Y_1^2 = F_0(X)F_2(X), \\ \mathcal{E}_2 &: Y_2^2 = F_0(X)F_1(X). \end{aligned} \tag{4.10}$$

In the sextic case, these will all be quartics in X, while in the quintic case we will have one quartic and two cubics. This will in fact be of no consequence for the general case.

Let us fix $d \in K^*$ such that F_1, F_2 are each defined over $K(\sqrt{d})$ [we take $d = 1$ for the case when they are defined over K]. Our aim is to find a 2-to-1 map $(X, y_0) \mapsto (v, w)$ from the above genus 1 curves to elliptic curves in the form $w^2 =$ (quadratic in v over K) $\times$ (linear in v over $K(\sqrt{d})$). Furthermore, we wish the map $X \mapsto v$ to be defined over K.

As in the previous section, let $T = \sigma(X)$, so $X = \sigma^{-1}(T)$. As we saw in the previous section, through this change of variable we get each F_i with only even powers of T modulo squares in the denominators which can be absorbed into the y_i^2. Both sides could now be multiplied by T^2 and then we replace T^2 by x on the right hand side, and absorb T^2 into the square of the left hand side, giving the elliptic curves in cubic form; for example the above $\mathcal{E}_1$ would then map to a curve of the form: **square** $= xF_{0x}(x)F_{2x}(x)$. However, the map $X \to x = \sigma(X)^2$ is not going to be K-rational in general,

and so we should not use this approach. Instead, we perform the following adjustment on x, to give v (a fractional linear transformation of x, which is defined over K.

Lemma 8. *Let $\mathcal{C}$ be as in (4.1), let $R, \sigma(X)$ as in Lemma 6, and $x = \sigma(X)^2$. Define v by:*

$$v = \sqrt{dR}\frac{x+1}{x-1},$$

which has inverse mapping

$$x = \frac{v+\sqrt{dR}}{v-\sqrt{dR}}.$$

Then $X \to v$ is a K-rational map.

Proof. Recall that $\sigma(X)$, and hence $x = \sigma(X)^2$, is defined over $K(\sqrt{dR})$. Furthermore, from the formulas in Lemma 6, which we rewrite (in the typical case – the other cases being similar) as:

$$\sigma(X) = \frac{\sqrt{R}(a_1b_2 - b_1a_2)X + \sqrt{R}(a_1c_2 - a_2c_1) - R}{\sqrt{R}(a_1b_2 - b_1a_2)X + \sqrt{R}(a_1c_2 - a_2c_1) + R},$$

and note that expressions such as $a_1b_2 - b_1a_2$ are of the form $\sqrt{d}k$ for some $k \in K$ (since a_1, a_2 are conjugate, as are b_1, b_2 and c_1, c_2). We can see that $\sqrt{dR} \mapsto -\sqrt{dR}$ swaps the numerator and denominator of $\sigma(X)$ and negates them. Hence $\sqrt{dR} \mapsto -\sqrt{dR}$ sends $\sigma(X)$ to $1/\sigma(X)$ and so sends $\sigma(X)^2$ to $1/\sigma(X)^2$; that is, x is sent to $1/x$. Hence $\frac{x+1}{x-1}$ is negated by $\sqrt{dR} \mapsto -\sqrt{dR}$, and so $v = \sqrt{dR}\frac{x+1}{x-1}$ is left invariant, giving that v is defined over K, as required. ∎

Note that we can invert $v = \sqrt{dR}\frac{x+1}{x-1}$ to give

$$x = \frac{v+\sqrt{dR}}{v-\sqrt{dR}}. \tag{4.11}$$

Just as in the previous section, if we replace X by $\sigma^{-1}(T)$ in $F_0(X)$, $F_1(X)$,

$F_2(X)$ of (4.2), we get

$$F_{1T}(T) = \frac{2a_1R(T^2+1) + (-2a_1a_2c_1 + 2a_1^2c_2 + a_2b_1^2 - b_1a_1b_2)\sqrt{R}(T^2-1)}{(a_1b_2 - a_2b_1)^2(T-1)^2}$$

$$F_{2T}(T) = \frac{2a_2R(T^2+1) + (-2a_2^2c_1 + 2a_2a_1c_2 - a_1b_2^2 + b_2a_2b_1)\sqrt{R}(T^2-1)}{(a_1b_2 - a_2b_1)^2(T-1)^2} \tag{4.12}$$

$$F_{0T}(T) = k_1F_{1T}(T) + k_2F_{2T}(T).$$

Now take $\mathcal{E}_1 : Y_1^2 = F_0(X)F_2(X)$, and substitute $X = \sigma^{-1}(T)$ so that the curve becomes $Y_1^2 = F_{0T}(T)F_{2T}(T)$, as above. Multiplying both sides by $\left(2Td(a_1b_2 - a_2b_1)^2/(T+1)^2\right)^2$ puts $\mathcal{E}_1$ in the form

$$y_1^2 = \left(2Td(a_1b_2 - a_2b_1)^2/(T+1)^2\right)^2 F_{0T}(T)F_{2T}(T), \tag{4.13}$$

where

$$y_1 = \frac{2Td(a_1b_2 - a_2b_1)^2}{(T+1)^2} = \frac{2\sigma(X)d(a_1b_2 - a_2b_1)^2}{(\sigma(X)+1)^2}. \tag{4.14}$$

The right hand side of (4.13), after simplifying, has only even powers of T. Replacing T^2 by x and then replacing x by $(v+\sqrt{dR})/(v-\sqrt{dR})$, as in (4.11), we see that (4.13) becomes:

$$y_1^2 = Q(v)L(v)M(v), \tag{4.15}$$

where

$$\begin{aligned}
Q(v) &= v^2 - dR, \\
L(v) &= 2(k_1a_1 + k_2a_2)v + (k_1A_1 + k_2A_2)\sqrt{d}, \\
M(v) &= 2a_2v + (-2a_2^2c_1 + 2a_1a_2c_2 - a_1b_2^2 + b_2a_2b_1)\sqrt{d}, \\
A_1 &= -2a_1a_2c_1 + 2a_1^2c_2 + a_2b_1^2 - b_1a_1b_2, \\
A_2 &= -2a_2^2c_1 + 2a_2a_1c_2 - a_1b_2^2 + b_2a_2b_1.
\end{aligned}$$

The map $(X, Y_1) \to (v, y_1)$ from $\mathcal{E}_1$ to (4.15) is given by

$$v = \sqrt{dR}\left(\frac{\sigma(X)^2+1}{\sigma(X)^2-1}\right) \text{ and } y_1 = \frac{2dY_1\sigma(X)(a_1b_2 - a_2b_1)^2}{(\sigma(X)+1)^2}.$$

Note that the quadratic $Q(v)$ and the linear $L(v)$ are defined over K, and the linear $M(v)$ is defined over $K(\sqrt{d})$. In order to see that $L(v)$ is defined over K, note that the action $\sqrt{d} \mapsto -\sqrt{d}$ also has the effect $k_1 \leftrightarrow k_2$, $a_1 \leftrightarrow a_2$, $b_1 \leftrightarrow b_2$, $c_1 \leftrightarrow c_2$, $A_1 \leftrightarrow -A_2$, and so $L(v)$ is left unchanged. As we have already mentioned, the map $X \mapsto v$ is defined over K (which is why we are using it, rather than the map $X \mapsto x$).

In order to put the curve (4.15) into the form **square** = cubic, we take the root v_0 of $L(v)$ and map it to infinity. Solving for the root of $L(v)$ gives

$$v_0 = -\frac{(k_1A_1 + k_2A_2)\sqrt{d}}{2(k_1a_1 + k_2a_2)}.$$

If we now map to $u = \frac{1}{v-v_0}$, with inverse $v = v_0 + \frac{1}{u}$, the effect will be to map the point $(v_0, 0)$ to infinity. Substituting $v = v_0 + \frac{1}{u}$ into (4.15) and multiplying both sides by $4(k_1a_1 + k_2a_2)^2u^4$ gives

$$\psi_1^2 = 4(k_1a_1 + k_2a_2)^2u^4Q\Big(v_0 + \frac{1}{u}\Big)L\Big(v_0 + \frac{1}{u}\Big)M\Big(v_0 + \frac{1}{u}\Big), \tag{4.16}$$

where

$$\psi_1 = 2y_1(k_1a_1 + k_2a_2)u^2, \quad u = \frac{1}{v - v_0}. \tag{4.17}$$

In detail, (4.16) gives

$$\mathcal{E}_1' : \psi_1^2 = Q(u)L_2(u), \tag{4.18}$$

where

$$\begin{aligned} Q(u) \;=\; & d(a_1b_2 - a_2b_1)^2(k_2^2b_2^2 + 2k_1b_1k_2b_2 - 4a_1c_1k_1^2 \\ & -4a_1k_1c_2k_2 - 4k_2^2a_2c_2 + k_1^2b_1^2 - 4c_1k_1k_2a_2)u^2 \\ & +4\sqrt{d}(k_1a_1 + k_2a_2)(2k_1a_1a_2c_1 - 2k_1a_1^2c_2 - k_1a_2b_1^2 \\ & +k_1b_1a_1b_2 - k_2b_2a_2b_1 - 2k_2a_2a_1c_2 + k_2a_1b_2^2 + 2c_1k_2a_2^2)u \\ & +4(k_1a_1 + k_2a_2)^2, \\ L_2(u) \;=\; & -2\sqrt{d}k_1(a_1b_2 - a_2b_1)^2u + 4a_2(k_1a_1 + k_2a_2). \end{aligned} \tag{4.19}$$

The map $(X, Y_1) \mapsto (u, \psi_1)$ is a 2-to-1 map from the genus 1 curve $\mathcal{E}_1$ to the elliptic curve $\mathcal{E}_1'$, and the map $X \mapsto u$ is defined over K. Similarly, the curve $\mathcal{E}_2$ (which is the conjugate of $\mathcal{E}_1$) maps to $\mathcal{E}_2'$, the conjugate of $\mathcal{E}_2$. Recall

that we want to determine all $(X, Y) \in \mathcal{E}_1(K(\sqrt{d}))$ such that $X \in K$. We have transformed that (using the strategy of Method 1) into the problem of finding all $(u, \psi_1) \in \mathcal{E}_1'(K(\sqrt{d}))$ such that $u \in K$. The problem of finding all $(u, \psi_2) \in \mathcal{E}_2'(K(\sqrt{d}))$ such that $u \in K$, is equivalent, since $\mathcal{E}_1'$ and $\mathcal{E}_2'$ are conjugate, and so we can just focus on $\mathcal{E}_1'$.

This completes the first step of the method, generalising that of [17].

4.2.2 The next genus 2 curve

In this section, we assume $d \neq 1$. The elliptic curve $\mathcal{E}_1'$ at the end of the last section, was of the form **square** $= q(u)l(u)$, where $q(u)$ is quadratic in u and defined over K, and $l(u)$ is linear in u and defined over $K(\sqrt{d})$. So we have the form:

$$\psi^2 = q(u)l(u), \tag{4.20}$$

defined over $K(\sqrt{d})$, and we wish to find all $K(\sqrt{d})$-rational points (u, ψ) for which $u \in K$. We shall find a new bielliptic genus 2 curve, defined over K, with the property that any such (u, ψ) gives rise to a K-rational point on the genus 2 curve. This genus 2 curve will turn out to have a 2-to-1 map to the elliptic curve $\psi^2 = q(u)l(u)$, with the map to u being K-rational. The conjugate map will be to the conjugate curve $\psi^2 = q(u)l'(u)$, where $l'(u)$ is the conjugate of $l(u)$.

Note that $l(u)$ will be of the form $l(u) = n_1(u) + n_2(u)\sqrt{d}$, where $n_1(u)$, $n_2(u)$ are linear and defined over K. In general we have

$$\begin{aligned} q(u) &= au^2 + bu + c, \\ n_1(u) &= i_1u + i_2, \\ n_2(u) &= j_1u + j_2. \end{aligned}$$

Now we let $\psi = r + s\sqrt{d}$ so that $(r + s\sqrt{d})^2 = q(u)(n_1(u) + n_2(u)\sqrt{d})$. We now equate the coefficient of $\sqrt{d}$ and the K-rational part, so that we have two equations in r, s.

$$2rs = q(u)n_2(u), \quad r^2 + ds^2 = q(u)n_1(u). \tag{4.21}$$

We can use the first equation to eliminate, say, r, using

$$r = \frac{q(u)n_2(u)}{2s} \tag{4.22}$$

and substitute this into the second equation, to give an equation in s which will be

$$\frac{q(u)^2 n_2(u)^2}{4s^2} + ds^2 - q(u)n_1(u) = 0. \tag{4.23}$$

Letting $t = s^2/q(u)$ we get

$$n_2(u)^2 + 4dt^2 - 4tn_1(u) = 0. \tag{4.24}$$

This describes a genus 0 curve. We now parametrise (4.24), using the base-point $(t_0, u_0) = (0, -j_2/j_1)$. The points (t, u) are then in 1-1 correspondence with the slope λ of the line through $(0, -j_2/j_1)$ and (t, u), that is: $\lambda = (u + j_2/j_1)/t$; instead of λ, we shall use the parameter $z = 1/(j_1\lambda) = t/(j_1u + j_2)$. Substituting $u = (t - j_2z)/(j_1z)$ into (4.24) [and recalling that $n_1(u) = i_1u + i_2, n_2(u) = j_1u + j_2$], we solve for t in terms of z, and substitute this into $u = (t - j_2z)/(j_1z)$ which also solves for u in terms of z. This gives the following parametrisation:

$$u(z) = \frac{-j_2 - 4dj_2z^2 + 4i_2z}{j_1 + 4j_1dz^2 - 4i_1z}, \quad t(z) = \frac{4z^2(i_2j_1 - i_1j_2)}{j_1 + 4dj_1z^2 - 4i_1z}. \tag{4.25}$$

In the special case when $j_1 = 0$, note that (4.24) is then linear in u, and so we can just take $z = t$ as our parameter and solve (4.24) for u. In this case we can take $u(z) = (j_2^2 + 4dz^2 - 4i_2z)/(4i_1z)$ and $t(z) = z$.

In either case, since $t = s^2/q(u)$, we see that there exists $z \in K$ such that $s^2 = t(z)q(u(z))$, giving a genus 2 curve in z, s, which is defined over K. Furthermore, the above shows that any $K(\sqrt{d})$-rational point on (4.20) with $u \in K$, give rise to a K-rational point on the genus 2 curve $s^2 = t(z)q(u(z))$. Also note that if (z, s) is a K-rational point on the genus 2 curve $s^2 = t(z)q(u(z))$, then $(z, s) \mapsto \big(u(z), q(u(z))n_2(u(z))/(2s) + s\sqrt{d}\big)$ gives a map to a point (u, ψ) on (4.20) [using the facts that $r = q(u)n_2(u)/(2s)$ and $\psi = r + s\sqrt{d}$], so that $s^2 = t(z)q(u(z))$ is bielliptic. This produces the new

bielliptic genus 2 curve, and completes one cycle of the process.

Letting $\underline{s} = sa(j_1 + 4j_1z^2d - 4zi_1)^2/z$ our genus 2 curve $s^2 = t(z)q(u(z))$ becomes (for the typical case when $j_1 \neq 0$):

$$\mathcal{C}' : \underline{s}^2 = G_0(z)G_1(z)G_2(z), \tag{4.26}$$

where

$$\begin{aligned} G_1(z) &= -2aj_2 - 8adj_2z^2 + 8ai_2z + bj_1 + 4bj_1dz^2 - 4bi_1z \\ &\quad +(j_1 + 4j_1dz^2 - 4i_1z)\sqrt{b^2 - 4ac}, \\ G_2(z) &= -2aj_2 - 8adj_2z^2 + 8ai_2z + bj_1 + 4bj_1dz^2 - 4bi_1z \\ &\quad -(j_1 + 4j_1dz^2 - 4i_1z)\sqrt{b^2 - 4ac}, \\ G_0(z) &= a(i_2j_1 - i_1j_2)(j_1 + 4j_1dz^2 - 4i_1z). \end{aligned} \tag{4.27}$$

Note also that

$$G_0(z) = \frac{a(i_2j_1 - i_1j_2)}{2\sqrt{b^2 - 4ac}}(G_1(z) - G_2(z)),$$

so that our new genus 2 curve has the same properties as our starting genus 2 curve: it is of the form $\underline{s}^2 = G_0(z)G_1(z)G_2(z)$, where G_0, G_1, G_2 satisfy the conditions of (4.2). This means that we can repeat the process described above where these new G_i are used instead of the F_i in the above demonstration.

Recall that, for the method to be successful, we need to be able to find all K-rational points either on $\mathcal{E}_0$ (the genus 1 curve defined over K) or on $\mathcal{C}'$ (our new genus 2 curve defined over K). For the former, we compute the rank of the elliptic curve, which is the Jacobian of $\mathcal{E}_0$. For the latter, we compute the 2-Selmer bound on the rank of $J'(K)$, where J' is the Jacobian of $\mathcal{C}$; if this is less than 2, then we can apply Chabauty's Theorem to try to find $\mathcal{C}'(K)$. Otherwise, we can attempt to apply the process again to $\mathcal{C}'$. In the next chapter, we shall find an example which cycles and defies repeated applications of the method.

Chapter 5

An example of cycling

In [17] the authors consider the curve $\mathcal{C} : Y^2 = (X^2+p)(X^4+p^2)$ over $\mathbb{Q}$ with $p \equiv 7 \bmod 8$ is some prime. Here however we extend their considerations by taking p to be any nonzero member of $\mathbb{Q}$ (that is, we have removed the congruence and primality conditions on the value).

Theorem 4. *When we apply Method 1, outlined in the previous chapter, to the curve*

$$\mathcal{C} : Y^2 = (X^2 + p)(X^4 + p^2),$$

for $0 \neq p \in \mathbb{Q}$, then there is a 4-cycle i.e. after 4 iterations of the method, following through the case D =identity, we return to the original curve.

Proof. This proof is rather long and so will be subdivided into mini-sections to make it flow pleasantly for the reader. In the first part of the proof we use the methods discussed previously to find the next genus 2 curve in the chain. The next part will involve using this genus 2 curve to produce another. In the final part of the proof we shall observe that this third genus 2 curve in the chain is birationally equivalent to the first over a quadratic number field and deduce from this the result stated in the theorem. In each case, we are applying the general methods of the previous chapter to the special case of each genus 2 curve; all of the genus 2 curves which arise in this chapter will be of the general form discussed in the last chapter, and so all of the general equations and techniques derived in the last chapter will apply here.

5.1 The second genus 2 curve in the chain

We start with $\mathcal{C}$ which factors into 3 quadratics as $Y^2 = (X^2+p)(X^2-pi)(X^2+pi)$ so we will take $\mathbb{Q}(i)$ as the required extension we will need. We set $F_0 = X^2+p$, $F_1 = X^2-pi$ and $F_2 = X^2+pi$. The resultant of F_1, F_2 with respect to X is $(-4p^2)$ and $k_1 = \frac{1}{2}+\frac{1}{2}i$, $k_2 = \frac{1}{2}-\frac{1}{2}i$. Note we can check to see that indeed $F_0 = k_1F_1 + k_2F_2$. Using the formula for $\tau(X)$ we obtain $-X$. Since $b_1 = b_2$ we are in Case 3 of Lemma 6 so $\sigma(X) = X$.

Focusing on the 3 genus one curves relating to the identity we have

$$\begin{aligned}
\mathcal{E}_0 &: \quad Y_0^2 = (X^4+p^2),\\
\mathcal{E}_1 &: Y_1^2 = (X^2+p)(X^2+pi),\\
\mathcal{E}_2 &: Y_2^2 = (X^2+p)(X^2-pi).
\end{aligned}$$

We now need to map $\mathcal{E}_1$ and $\mathcal{E}_2$ to a curve of the required form described in the previous chapter (**square** = (quadratic in $\mathbb{Q}$)(linear in $\mathbb{Q}(i)$)). Using the substitution which gives the curves in even powers of T gives

$$\begin{aligned}
\mathcal{E}_1 &: Y_1^2 = (T^2+p)(T^2+pi),\\
\mathcal{E}_2 &: Y_2^2 = (T^2+p)(T^2-pi).
\end{aligned}$$

and we can multiply each of these by T^2 and substituting x for T^2 to give a map $(T, Y_i) \mapsto (T^2, TY_i)$ from $\mathcal{E}_i$ to $\underline{\mathcal{E}}_i$, where:

$$\begin{aligned}
\underline{\mathcal{E}}_1 &: \psi_1^2 = x(x+p)(x+pi),\\
\underline{\mathcal{E}}_2 &: \psi_2^2 = x(x+p)(x-pi).
\end{aligned}$$

These curves are already of the required form, and the map $X \to x = \sigma(X)^2 = X^2$ is already $\mathbb{Q}$-rational. Note that this example is in fact unusual as we have already noted that the map $X \to \sigma(X)^2$ is not normally $\mathbb{Q}$-rational. In order to be systematic we show how the elliptic curves transform when we adhere to the steps described in the general case. Note that, in the notation of the previous section, we can take $d = -1$ (since F_1, F_2 are defined over $\mathbb{Q}(\sqrt{d})$ and $R = \text{resultant}(F_1, F_2) = -4p^2$, so that $dR = 4p^2$. Hence, by Lemma 7, $\sigma(X) \in \mathbb{Q}$. Therefore we should now change from x to v by the

substitution

$$x = \frac{v + 2p}{v - 2p}$$

(from the formula in Lemma 8, adjusted by $2p$). Substituting into $\mathcal{E}_1$, and multiplying through by $(v - 2p)^4$ (which can be absorbed into the square), gives

$$\textbf{square} = (v + 2p)(v - 2p)(v + vp + 2p - 2p^2)(v + 2p + ipv - 2ip^2),$$

where the linear factor $(v + vp + 2p - 2p^2)$ arose from $x + p$, which in turn arose from $F_0 = X^2 + p$. The general strategy tells us to find the root v_0 of the factor $(v + vp + 2p - 2p^2)$, that is

$$v_0 = \frac{2p(p-1)}{p+1},$$

and then to map to $\underline{u} = 1/(v - v_0)$. Substituting $v = 1/\underline{u} + v_0$ and multiplying through by $\underline{u}^4(p+1)^2$, which gets absorbed into the square, gives

$$\textbf{square} = (4p^2\underline{u} + p + 1)(4p\underline{u} - p - 1)(4p^2(-1+i)\underline{u} - (p+1)(1+ip)).$$

We now perform the linear change in variable $\underline{u} = -(p+1)((p+1)u+p)/(4p^3)$, which gives

$$\mathcal{E}_1' : \underline{\psi}_1^2 = u(u+p)((1-i)u - ip).$$

Similarly for $\mathcal{E}_2$ we get

$$\mathcal{E}_2' : \underline{\psi}_2^2 = u(u+p)((1+i)u + ip).$$

Here each $\underline{\psi}_i = \psi_i(u+p)^2/p^2$. Since the two models of $\mathcal{E}_1'$ and $\mathcal{E}_2'$ are conjugate, we will expect, after step two, that the resulting genus 2 curve over $\mathbb{Q}$ should be the same (up to birational equivalence) either way. Still it doesn't do any harm to follow it through using both versions.

Using $\underline{\mathcal{E}}_1$ in the variable x, we have $q = x(x+p)$ and $l = x + pi$. We have $d = -1$ and can let $\psi_1 = r + si$. Taking imaginary and real parts gives two equations $2rs = px^2 + xp^2$ and $r^2 - s^2 = x^3 + px^2$. Solving the

first of these equations for r, substituting this into the second equation, and letting $t = s^2/(x(x+p))$, gives $4tx = p^2 - 4t^2$. To match with the discussion preceding (4.25) in the previous chapter, note that we are using x here rather than u; what was called $n_1(x) = i_1x + i_2$ in the previous chapter is here: $n_1(x) = x$, so that $i_1 = 1, i_2 = 0$, and $n_2(x) = j_1x + j_2 = p$, so that $j_1 = 0, j_2 = p$. Since $j_1 = 0$, we do not use (4.25); since $4tx = p^2 - 4t^2$, we could simply (as in the discussion immediately after (4.25)) set $t(z) = z$ and solve for x; however, it will simplify the next step if we instead take $t(z) = (z + 2p)/4$ and solve for x to give

$$x(z) = -\frac{z}{4}\frac{(z+4p)}{(z+2p)}.$$

The new genus 2 curve is then

$$s^2 = t(z)q(x(z)) = \frac{z(z+4p)(z^2-8p^2)}{64(z+2p)}.$$

Taking $\underline{s} = 8(z+2p)s$ then gives

$$\underline{s}^2 = z(z+2p)(z+4p)(z^2-8p^2).$$

In the next application we should take as our new F_0 the G_0 here, which relates to the factor coming from $t(z)$, so will be $x + 2p$. Now recall that our original q factors as $x(x+p)$ (of course for a typical example, this will factor over a quadratic field extension). Then G_1 and G_2, our new F_1 and F_2, arise from these factors x and $x+p$. Therefore $G_1 = z^2 - 8p^2$ and $G_2 = z(z+4p)$.

Using $\mathcal{E}_1'$ in the variable u, we have $q = u(u+p)$ and $l = (1-i)u - pi$ [we shall use q, l as shorthand for $q(u), l(u)$, respectively]. To match with the discussion preceding (4.25) in the previous chapter, what was called $n_1(u) = i_1u + i_2$ in the previous chapter is here: $n_1(u) = u$, so that $i_1 = 1, i_2 = 0$, and $n_2(u) = j_1u + j_2 = -u - p$, so that $j_1 = -1, j_2 = -p$; furthermore, $d = -1$. Letting $\underline{\psi}_1 = r + si$ and taking imaginary and real parts, we get two equations $2rs = -u^3 - 2pu^2 - p^2u$ and $r^2 - s^2 = u^3 + pu^2$. Using the first of these to solve for r, substituting this into the second, and then letting $t = s^2/(u(u+p))$,

gives the equation $4tu = p^2+2pu-4t^2+u^2$ (our genus 0 curve, which we shall now parametrise). Since $j_1 \neq 0$, we can take $\underline{z} = t/(j_1u + j_2) = -t/(u + p)$ as our parameter and directly apply the general formulae from (4.25) to give the parametrisation:

$$u(\underline{z}) = -\frac{p(4\underline{z}^2 - 1)}{4\underline{z}^2 - 4\underline{z} - 1}$$

and

$$t(\underline{z}) = \frac{4p\underline{z}^2}{4\underline{z}^2 - 4\underline{z} - 1}.$$

Our new genus 2 curve is

$$s^2 = t(\underline{z})q(u(\underline{z})) = 16p^3\underline{z}^3(4\underline{z}^2 - 1)/(4\underline{z}^2 - 4\underline{z} - 1)^3.$$

Now, let $z = 4p\underline{z} - 2p$, so that $\underline{z} = (z + 2p)/(4p)$, giving:

$$s^2 = \frac{4p^4z(z + 2p)^3(z + 4p)}{(z^2 - 8p^2)^3}.$$

Taking $\underline{s} = s(z^2 - 8p^2)^2/(2p^2(z + 2p))$ then gives:

$$\underline{s}^2 = z(z + 2p)(z + 4p)(z^2 - 8p^2),$$

which is the same genus 2 curve as before (regardless of whether $\underline{\mathcal{E}}_1$ or $\mathcal{E}_1'$ is used, we get the same genus 2 curve). Taking our G_0 as the factor coming from $t(z)$ will mean $G_0 = z^2 - 8p^2$. The others, G_1 and G_2, come from how q factors. We can see that $G_1 = z + 2p$ and $G_2 = z(z + 4p)$.

This is a complete cycle. In [17], the authors got to this stage. It would have been difficult using the approach of the authors, to proceed any further, since from now on we need to use the general method because $\sigma(X)^2$ for the next stage is not defined over $\mathbb{Q}$. The two versions $\underline{\mathcal{E}}_1$ or $\mathcal{E}_1'$ give rise to exactly the same genus 2 curve: square $= z(z + 2p)(z + 4p)(z^2 - 8p^2)$, and the same 3 at-most-quadratic factors: $z^2 - 8p^2$, $z + 2p$, $z(z + 4p)$. The first version $\underline{\mathcal{E}}_1$ is the version that [17] implied, whereas the other version comes from algebra relating to the general method. The only difference is that the version in [17] implied that the choice of G_0 (for the next cycle) should be

$z+2p$, whereas the systematic approach suggests that G_0 should be z^2-8p^2. We will adopt this latter version for the rest of the proof. At this point we have completed one full cycle and are ready to start a new cycle with $F_0 = X^2 - 8p^2$, $F_1 = X + 2p$ and $F_2 = X(X + 4p)$.

In summary, for the method to be successful after one application, we need to be able to find (to satisfy just the case where D is the identity) all $\mathbb{Q}$-rational points on the genus 1 curve $\mathcal{E}_0 : Y_0^2 = X^4 + p^2$, and all $\mathbb{Q}$-rational points on the genus 2 curve $s^2 = z(z + 2p)(z + 4p)(z^2 - 8p^2)$. Note that the map $(X, Y_0) \mapsto (X^2, XY_0)$ is a 2-covering from $\mathcal{E}_0$ to the elliptic curve:

$$H_1 : y^2 = x(x^2 + p^2).$$

Strictly speaking (in general), we are interested in the rank of the Mordell-Weil group of the Jacobian of $\mathcal{E}_0$. However this Jacobian is 2-isogenous to H_1, so that the rank of $H_1(\mathbb{Q})$ is the same as the rank of $\mathcal{E}_0(\mathbb{Q})$; so, we might as well use H_1 since it is in cubic form. For future reference, we shall also let H_2 denote this new genus 2 curve:

$$H_2 : Y^2 = X(X + 2p)(X + 4p)(X^2 - 8p^2).$$

One application of the method fails if the 2-Selmer bound of the rank of $H_1(\mathbb{Q})$ is nonzero, and the 2-Selmer bound on the rank of the Mordell-Weil group of the Jacobian of H_2 is at least 2.

5.2 The next cycle in the chain, calculating the third curve of genus 2

For this next cycle, all of the factors $F_0 = X^2 - 8p^2$, $F_1 = X + 2p$ and $F_2 = X(X+4p)$, in the hyperelliptic equation, are defined over $\mathbb{Q}$. The resultant of F_1, F_2 with respect to X is $-4p^2$, and $F_0 = k_1F_1+k_2F_2$, where $k_1 = -4p, k_2 = 1$. The formula for τ in Lemma 5 gives $\tau = \frac{-2p(X+4p)}{X+2p}$ and similarly Lemma 6 gives $\sigma(X) = \frac{X+2p+2pi}{X+2p-2pi}$. Focusing on the 3 elliptic curves which relate to the

identity give

$$\begin{aligned}\mathcal{E}_0 &: \quad Y_0^2 = (X+2p)X(X+4p),\\ \mathcal{E}_1 &: \quad Y_1^2 = (X^2-8p^2)X(X+4p),\\ \mathcal{E}_2 &: \quad Y_2^2 = (X^2-8p^2)(X+2p).\end{aligned}$$

These are all defined over $\mathbb{Q}$ and so here we have $d = 1$ so the quadratic extension $\mathbb{Q}(\sqrt{d})$ is just $\mathbb{Q}$. We will therefore look to map $\mathcal{E}_1$ and $\mathcal{E}_2$ to curves of the form square = (quadratic in $\mathbb{Q}$)(linear in $\mathbb{Q}$) and such that the map on the $x-$coordinate is $\mathbb{Q}$-rational. Firstly we set $T = \sigma(X)$, so want $X = \sigma^{-1}(T)$. This will be the substitution to take the curves to equations with only even powers of T. This is computed as $X = \frac{2p(1-T+i+iT)}{T-1}$. Substituting $X = \frac{2p(1-T+i+iT)}{T-1}$ into $\mathcal{E}_1, \mathcal{E}_2$ (the important pieces for computing the next genus 2 curve) gives

$$Y_1^2 = 64p^4(1+i)(T^2-i)(T^2+1)/(T-1)^4,$$

$$Y_2^2 = 16p^3(1-i)(T^2-i)(T+1)/(T-1)^3.$$

We multiply both sides of $\mathcal{E}_1$ by $T^2(T-1)^4/(64p^4)$, and absorb this into the square on the left hand side. Similarly, we multiply both sides of $\mathcal{E}_2$ by $T^2(T-1)^4/(16p^2)$ and absorb this into the square on the left hand side. This transforms $\mathcal{E}_1, \mathcal{E}_2$ to:

$$\begin{aligned}\textbf{square} &= (1+i)T^2(T^2-i)(T^2+1),\\ \textbf{square} &= (1-i)pT^2(T^2-i)(T^2-1),\end{aligned}$$

and so, after our usual substitution of x for T^2, we have:

$$\begin{aligned}\textbf{square} &= (1+i)x(x-i)(x+1),\\ \textbf{square} &= (1-i)px(x-i)(x-1).\end{aligned}$$

However, the x-coordinate map, $X \to x = \sigma(X)^2$ is not $\mathbb{Q}$-rational. We are compelled to use the further mobius transformation to make it $\mathbb{Q}$-rational. That is, use $v = \sqrt{dR}(x+1)/(x-1)$, given in Lemma 8 for the general case. Here, $d = 1$ and $R = \text{resultant}(F_1, F_2) = -4p^2$, so that our mapping is $v = 2pi(x+1)/(x-1)$ which has inverse mapping given by $x = (v+2pi)/(v-2pi)$.

Making this substitution transforms the above to:

$$\begin{aligned}\textbf{square} &= 4(v-2p)(v+2pi)v/(v-2pi)^3,\\ \textbf{square} &= 8p^2(v-2p)(v+2pi)/(v-2pi)^3.\end{aligned}$$

The linear factor $(v-2p)$ arose from $(x-i)$. We thus have $v_0 = 2p$. As in the discussion immediately preceding (4.16), we map to $\underline{u} = \frac{1}{v-v_0}$ with inverse $v = v_0 + \frac{1}{\underline{u}}$. Making this substitution gives:

$$\begin{aligned}\textbf{square} &= -8(2p\underline{u}+1)(4p\underline{u}+1-i)/(4p\underline{u}+1+i)^3,\\ \textbf{square} &= -16p^2\underline{u}(4p\underline{u}+1-i)/(4p\underline{u}+1+i)^3.\end{aligned}$$

We now make the linear change $\underline{u} = (u-p)/(4p^2)$, with inverse $u = 4p^2\underline{u}+p$, which gives:

$$\begin{aligned}\textbf{square} &= -4(iu+p)p(u+p)/(-iu+p)^3,\\ \textbf{square} &= -4p^2(iu+p)(u-p)/(-iu+p)^3.\end{aligned}$$

We multiply both sides of the first equation by $i^2(-iu+p)^4/4$, and absorb this into the square on the left hand side. Similarly, we multiply both sides of the second equation by $i^2(-iu+p)^4/(4p^2)$, and absorb this into the square on the left hand side. This gives:

$$\mathcal{E}_1' : \psi_1^2 = (u^2+p^2)p(u+p),$$

$$\mathcal{E}_2' : \psi_2^2 = (u^2+p^2)(u-p).$$

If we compose the above maps, we obtain the map from $\mathcal{E}_1$ to $\mathcal{E}_1'$ given by:

$$(X, Y_1) \mapsto \big(p(X^2+8pX+8p^2)/(X^2-8p^2), 2p^2Y_1(X^2+4pX+8p^2)/(X^2-8p^2)^2\big),$$

and the map from $\mathcal{E}_2$ to $\mathcal{E}_2'$ given by:

$$(X, Y_2) \mapsto \big(p(X^2+8pX+8p^2)/(X^2-8p^2), 4p^2Y_2(X^2+4pX+8p^2)/(X^2-8p^2)^2\big).$$

Note that both maps are defined over $\mathbb{Q}$. Here the (u^2+p^2) is the common quadratic right hand sides of the above models of $\mathcal{E}_1'$ and $\mathcal{E}_2'$ whereas $p(u+p)$ and $(u-p)$ are the 'conjugate' linear factors of the right hand sides, over $\mathbb{Q}$ in the sense described in the next paragraph.

At this next stage we have $q = u^2+p^2$ and $l = p(u+p)$. We want to compute n_1 and n_2 such that $l = n_1 + \sqrt{d}n_2$, which in the last case was the real and imaginary parts [again, we are using q, l, n_1, n_2 as shorthand for $q(u), l(u), n_1(u), n_2(u)$, respectively]. Here, however, we must be careful as $d = 1$. This is however rather simple to get around since we just need to choose n_1, n_2 to be the unique linear polynomials in u such that $n_1+\sqrt{d}n_2 = p(u+p)$ [the linear factor of the right hand side of $\psi_1^2 = (u^2+p^2)p(u+p)$] and $n_1 - \sqrt{d}n_2 = u-p$ [the linear factor of the right hand side of $\psi_2^2 = (u^2+p^2)(u-p)$], namely: $n_1 = \frac{l+(u-p)}{2} = \frac{(p+1)u+p(p-1)}{2}$ and $n_2 = \frac{(p-1)u+p(p+1)}{2}$. That is to say, we have chosen n_1, n_2 such that $n_1 + \sqrt{d}n_2 = n_1 + n_2$ is the linear portion (after removing u^2+p^2) of the right hand side of our equation for $\mathcal{E}_1'$, and $n_1 - \sqrt{d}n_2 = n_1 - n_2$ is the linear portion (after removing u^2+p^2) of the right hand side of our equation for $\mathcal{E}_2'$. In the notation of the previous chapter (preceding (4.25)) we have $i_1 = (p+1)/2, i_2 = p(p-1)/2, j_1 = (p-1)/2, j_2 = p(p+1)/2$. Note that, even when $d = 1$, we can still proceed as if equating coefficients of 1 and d, using the above n_1, n_2, since the formulas still give a curve of genus 2 with maps to $\mathcal{E}_1', \mathcal{E}_2'$, provided that n_1, n_2 have been chosen so that $n_1 + \sqrt{d}n_2$ gives the linear factor of $\mathcal{E}_1'$ and $n_1 - \sqrt{d}n_2$ gives the linear factor of $\mathcal{E}_2'$.

Next we do the substitution $\psi_1 = r + \sqrt{d}s = r + s$. Obtaining two equations in r, s we again can eliminate r and letting $t = s^2/(u^2+p^2)$, we obtain our genus 0 curve, which is $n_2^2 + 4t^2 = 4tn_1$. We wish to parametrise this, so using the general formula (4.25) of the previous chapter, we get

$$u(\underline{z}) = \frac{-p(4p\underline{z}^2 + p - 4p\underline{z} + 1 + 4\underline{z}^2 + 4\underline{z})}{4p\underline{z}^2 - 4p\underline{z} + p - 4\underline{z}^2 - 1 - 4\underline{z}}$$

and

$$t(\underline{z}) = \frac{-8p^2\underline{z}^2}{4p\underline{z}^2 - 4p\underline{z} + p - 4\underline{z}^2 - 1 - 4\underline{z}}.$$

Our genus 2 curve for the next cycle will therefore be

$$\begin{aligned} s^2 = t(\underline{z})q(u(\underline{z})) = \; & -16p^4\underline{z}^2(1+p^2+8\underline{z}+24p^2\underline{z}^2-8p^2\underline{z}+16p^2\underline{z}^4 \\ & -32p^2\underline{z}^3+24\underline{z}^2+16\underline{z}^4+32\underline{z}^3)/ \\ & (p-1+4p\underline{z}^2-4\underline{z}^2-4p\underline{z}-4\underline{z})^3. \end{aligned}$$

Letting $\underline{z} = \frac{1}{2}(z-1)/(z+1)$ gives:

$$s^2 = p^4(z-1)^2(z^4+p^2)/(z^2-p)^3.$$

Multiplying both sides by $(z^2-p)^4/(p^4(z-1)^2)$ and letting

$$\underline{s} = s(z^2-p)^2/(p^2(z-1))$$

then gives

$$\underline{s}^2 = (z^4+p^2)(z^2-p).$$

Therefore, the curve $Y^2 = (X^4+p^2)(X^2-p)$ is the next genus 2 curve in our sequence. Note that the map $(X,Y) \to (X^2,Y)$ is from this curve to $\mathcal{E}_2'$, while the map $(X,Y) \to (-p^2/X^2, pY/X^3)$ is from this curve to $\mathcal{E}_1'$. Thus this genus 2 curve will be the one used in the next cycle.

For future reference, we shall label $\mathcal{E}_0$ as H_3; that is:

$$H_3 : y^2 = (x+2p)x(x+4p).$$

This is already of cubic form, and so can be left as it is. For future reference, we shall also let H_4 denote our new genus 2 curve:

$$H_4 : Y^2 = (X^4+p^2)(X^2-p).$$

One second application of the method fails if the 2-Selmer bound of the rank of $H_3(\mathbb{Q})$ is nonzero, and the 2-Selmer bound on the rank of the Mordell-Weil group of the Jacobian of H_4 is at least 2.

5.3 Final stage, cycling is clear

So, after starting with $Y^2 = (X^4 + p^2)(X^2 + p)$, and performing two cycles, we get $Y^2 = (X^4 + p^2)(X^2 - p)$. Of course, geometrically, we are now back to the original curve, since $(X, Y) \to (iX, iY)$ is a birational transformation between $Y^2 = (X^4 + p^2)(X^2 + p)$ and $Y^2 = (X^4 + p^2)(X^2 - p)$. So, after two complete cycles we are back to a curve which is birationally equivalent over $\mathbb{Q}(i)$, but not over $\mathbb{Q}$. This curve after two applications is the same as the original, but with p replaced by $-p$. If we let q denote $-p$, then after two cycles the original becomes $Y^2 = (X^4 + q^2)(X^2 + q)$. So a further two cycles will take it to $Y^2 = (X^4 + q^2)(X^2 - q)$, which is just $Y^2 = (X^4 + p^2)(X^2 + p)$.

So repetition must indeed occur in 4 cycles. ∎

5.4 Summary of the curves from Theorem 4

We can summarise the above example. Starting with the bielliptic genus 2 curve $\mathcal{C} : Y^2 = (X^2 + p)(X^4 + p^2)$, then

First cycle gives	:	$H_1 : y^2 = x(x^2 + p^2)$
New genus 2 curve	:	$H_2 : Y^2 = X(X + 2p)(X + 4p)(X^2 - 8p^2)$
Second cycle gives	:	$H_3 : y^2 = (x + 2p)x(x + 4p)$
New genus 2 curve	:	$H_4 : Y^2 = (X^2 - p)(X^4 + p^2)$
Third cycle gives	:	$H_5 : y^2 = x(x^2 + p^2)$
New genus 2 curve	:	$H_6 : Y^2 = X(X - 2p)(X - 4p)(X^2 - 8p^2)$
Fourth cycle gives	:	$H_7 : y^2 = (x - 2p)x(x - 4p)$
New genus 2 curve	:	$H_8 = \mathcal{C} : Y^2 = (X^2 + p)(X^4 + p^2)$

and so repetition.

5.4.1 Some notes and values of p

In [17], the authors concerned themselves with ensuring that this method always provided a way to resolve $\mathcal{C}(\mathbb{Q})$. This proves possible for p a prime

such that $p \equiv 7 \bmod 16$. We have, for the general case, the fact that $p \in \mathbb{Q}$. A counterexample to the method for determining all $\mathbb{Q}$ points on $Y^2 = (X^2+p)(X^4+p^2)$, would be a rational value of p where each of the $\mathcal{E}_0$ have (Mordell-Weil group of the Jacobian) rank at least 1 and all of the genus 2 curves in the cycle have Mordell-Weil group of the Jacobian of rank at least 2. In fact, it is even of interest if we can find rational p where the Selmer bounds are at least this large.

Theorem 5. *The* **Method** *fails (in the 2-Selmer bound version) for each of* $p = 31,47,79$, *with* $p < 100$, *regardless of however many times the method is repeatedly applied.*

Proof. Since we have been concerned with the identity case (which must be involved), we merely need to show that the Selmer bounds for $p = 31, 47, 79$ each of the curves $H_1, \ldots, H_8$ are, for the elliptic curves $(H_1, H_3, H_5, H_7) \geq 1$ and for the Jacobians of the genus 2 curves $(H_2, H_4, H_6, H_8) \geq 2$, too high for Chabauty to apply. The computer packages used were [38] and [40]. We give below the table of these bounds.

Curve :	Rank or Selmer bound over $\mathbb{Q}$ for		
	$p = 31$	$p = 47$	$p = 79$
H_1	**1**	**1**	**1**
H_2	*2*	*2*	*2*
H_3	**1**	**1**	**1**
H_4	*3*	*3*	*3*
H_5	**1**	**1**	**1**
H_6	*2*	*2*	*2*
H_7	**1**	**1**	**1**
H_8	*2*	*2*	*2*

∎

Entries in **bold** are actual ranks, while those in *italics* are the Selmer bounds where it has proved impossible to find points (and so improve from a bound to an actual rank).

Conjecture 2. *The method described always fails for integer prime p, with $p \equiv 15$ mod 16.*

Evidence to support Conjecture 2. It seems reasonable that, as can be seen in the above table, since ALL of the Selmer bounds (or actual ranks) for each of the respective curves are the same regardless of whether we consider $31, 47$ or 79 for the different curves, to theorise that this will be a feature for primes p of this type.

Appendix A

Second Descent of an elliptic curve, adapted from [37]

Here I set out the procedure of 2nd-descent, which can be helpful in determining the rank of an elliptic curve. We have

$$\mathcal{C} : y^2 = x(x^2 + ax + b),\ \widehat{\mathcal{C}} : y^2 = x(x^2 + a_1x + b_1)\ a, b \in \mathbb{Z},$$

where

$$a_1 = -2a, b_1 = a^2 - 4b.$$

$\mathcal{C}$ and $\widehat{\mathcal{C}}$ are 2-isogenous curves. Suppose that we have not been able to find a rational point on the locally solvable homogeneous space

$$rv^4 + av^2 + \frac{b}{r} = u^2.$$

The following is known as **second descent**. Since the quartic is locally solvable, then by the Hasse principle, the associated quadratic

$$rw^2 + aw + \frac{b}{r} = u^2$$

does have a rational point, say (u_0, w_0). We note that w_0 will not occur since then $\frac{b}{r}$ is a square. All rational points on the quadratic are given

parametrically by

$$w = \frac{w_0 t^2 - 2u_0 t + a + r w_0}{t^2 - r} =: \frac{f(t)}{g(t)},$$

$$u = \frac{-u_0 t^2 + (a + 2r w_0)t - u_0 r}{t^2 - r}.$$

Letting @ denote (various) rational squares, we wish to find $w = @$, i.e. we seek $t \in \mathbb{Q}$ such that

$$f(t) = d * @ \text{ and } g(t) = d * @$$

for some non-zero squarefree $d \in \mathbb{Z}$. Let k denote the denominator of w_0. Since $u_0^2 = r w_0^2 + a w_0 + \frac{b}{r}$, therefore $k u_0 \in \mathbb{Z}$, hence $kf \in \mathbb{Z}[t]$. It follows that

$$R := \text{ resultant } (kf, kg) = k^4 b_1.$$

Suppose that $t = t_1/t_2$, $\gcd(t_1, t_2) = 1$ is a solutions to $f(t)$ and $g(t)$ above, then

$$t_2^3 k^4 b_1 \in \mathbb{Z}$$

Thus we have $dn = t_2^3 k^4 b_1$ from some $n \in \mathbb{Z}$. Now d is square-free, also $t_2^2 g(t) = t_1^2 - r t_2^2 = d * @$ and $\gcd(t_1, t_2) = 1$. It follows that no prime dividing d divides t_2 and therefore d divides $k b_1$. Thus we obtain a finite list of candidates d.

Consider first the special case of $d = 1$. The homogeneous form of the equation $t^2 - r = s^2$ is $T^2 - rU^2 = S^2$ with solution $(T, U, S) = (1, 0, 1)$. The general solution is

$$(d = 1)\ t = \frac{\tau^2 + r}{2\tau}, \tau \text{ a parameter.}$$

In general, since $g(t) = d * @$ implies an equation of the form

$$dt^2 - dr = s^2, \tag{A.1}$$

we have the norm residue conditions

$$(d, dr)_p = 1 \text{ for } p = \infty \text{ and all prime divisors of } dr,$$

which may eliminate some $d \neq 1$.

Suppose now that $d \neq 1$ and that d survives the norm residue conditions so that there is a solution (s_0, t_0) of (A.1). (The homogeneous equation $dT^2 - drU^2 = S^2$ does not have a solution with $U = 0$ since d is not a square.) If it happens that $f(t_0) = d * @$, then the procedure is done - we have found a rational point on the original quartic. Otherwise we look at the general solution

$$(d \neq 1)\ t = \frac{t_0\tau^2 - 2s_0\tau + dt_0}{\tau^2 - d}, \tau \text{ a parameter.}$$

Since we want $f(t) = d * @$, clearing denominators and substituting for t , we seek a value of τ such that, respectively,

$$4\tau^2 f(t) = @ \text{ or } d(\tau^2 - d)^2 f(t) = @.$$

Thus we obtain a list of one or more equations of the form

$$\text{quartic in } \tau = @.$$

These equations are called the **descendant quartics**. The procedure now is to eliminate the descendant quartics that are not everywhere locally solvable, that is not solvable in $\mathbb{R}$ or some $\mathbb{Q}_p$. If none survive then the original quartic has no rational points – the homogeneous space is not elliptic - and the procedure is done.

Appendix B

Computer Programs

B.1 Computer code

B.1.1 A procedure to print out the genus 2 covers related to solving Fermat Quartics from Chapter 2

```
#
#Maple code for computing the 3 covers
#associated to Fermat Quartics as outlined
#in Chapter 2
#
restart:
cov:=proc(a,b)
#Input the values of a,b where c=a^4+b^4
global c,d,e1,e2,g11,g12,
g13,g21,g22,g23,g31,g32,
cov1,cov2,cov3,l1,l2,l3,l4,l5,x,y;
#The variables are made global in order to
#manipulate them after each application of cov
c:=a^4+b^4; #Defines c
d:=x^4+y^4=a^4+b^4; #Defines the quartic curve
print(d); # We print the curve being considered
```

```
e1:=y^2=x^3-c*x; e2:=y^2=x^3+c^2*x;
#d is isogenous to e1xe1xe2
print(e1); print(e2);
#These are the elliptic curves printed
g11:=(a+b)^2*x^2-4*(a^2+a*b+b^2)*x+2*(a+b)^2;
g12:=(a-b)^2*x^2+4*(a^2-a*b+b^2)*x+2*(a-b)^2;
g13:=x^2-2;
cov1:=y^2=g11*g12*g13;
#g11,g12,g13 are shown in [17]
print(cov1); #The first of the 3 covers
g21:=a^2*x^2-2*b^2*x-a^2;
g22:=b^2*x^2+2*a^2*x-b^2;
g23:=x^2+1;
cov2:=y^2=g21*g22*g23;
print(cov2); #g21,g22,g23 are found by imitating
#the argument from [17]
l1:=a^4+2*a^2*b^2+b^4;
l2:=8*a*b^3-8*a^3*b;
l3:=12*(a^4-2*a^2*b^2+b^4);
l4:=16*a^3*b-16*a*b^3;
l5:=4*(a^4+2*a^2*b^2+b^4);
g31:=l1*x^4+l2*x^3+l3*x^2+l4*x+l5;
g32:=x^2+2;cov3:=y^2=g31*g32; print(cov3);
#The final cover, again found
#by imitating the argument from [17]
end proc;
```

B.1.2 Maple code to verify Lemma 6

```
#Here we use maple commands to verify that the 3 versions
#of sigma are negated by tau (the involution)
#and whose square is invariant
#We assign tau as given in Lemma 5
```

```
#sig1 is case 1 sigma from Lemma 6
#sig2 is case 2 sigma from Lemma 6
#sig3 is case 3 sigma from Lemma 6
F1:=a1*X^2+b1*X+c1;
F2:=a2*X^2+b2*X+c2;
tau := ((a1*c2-a2*c1)*X + b1*c2-b2*c1)
/((a2*b1-a1*b2)*X + a2*c1-a1*c2);
sig1 :=
((a1*b2-a2*b1)*X+a1*c2-a2*c1-sqrt(resultant(F1,F2,X)))/
((a1*b2-a2*b1)*X+a1*c2-a2*c1+sqrt(resultant(F1,F2,X)));
sig2 :=
((a1*c2-a2*c1+sqrt(resultant(F1,F2,X)))*X+b1*c2-b2*c1)/
((a1*c2-a2*c1-sqrt(resultant(F1,F2,X)))*X+b1*c2-b2*c1);
sig3 := X;
check1 := simplify( sig1 + subs(X=tau, sig1) );
#Gives 0
check2 := simplify( sig2 + subs(X=tau, sig2) );
#Gives 0
check3 := simplify( sig3 + subs(X=tau, sig3) );
#Gives an expression which is of course 0
#when we use the conditions a1*b2-b1*a2=0 and
#b1*c2-c1*b2=0
#So indeed each of the potential sigma are negated
#by tau
#
#Note that invariance is immediate in all cases
#of sigma due to this negation of sigma by tau
#This helps completes the proof of Lemma 6.
```

B.1.3 Maple code relating to cycling effect studied in Chapters 4,5

```
interface(prettyprint, prettyprint=false);
mob:=(a*X+b)/(c*X+d);
solve({subs(X=r1,mob)=s1,subs(X=s1,mob)=r1,
subs(X=r2,mob)=s2,subs(X=s2,mob)=r2},{a,b,c,d});
mob1:=simplify(subs(\%, mob));
#The result is:
#mob1 :=
#( (r1*s1 - r2*s2)*X + (r1 + s1)*r2*s2 - r1*s1*(r2 + s2) )/
#( ((r1 + s1) - (r2 + s2))*X + r2*s2 - r1*s1 );
#The follows gives 0,
#showing that the above is the same as mob1:
check := mob1 -
( (r1*s1 - r2*s2)*X + (r1 + s1)*r2*s2 - r1*s1*(r2 + s2) )/
( ((r1 + s1) - (r2 + s2))*X + r2*s2 - r1*s1 );
simplify(\%);
#
# Now, if:
F1 := a1*X^2 + b1*X + c1;
F2 := a2*X^2 + b2*X + c2;
# and if r1,s1 are the roots of F1
#and r2,s2 are the roots of F2,
# then a1*X^2 + b1*X + c1 = a1*(X - r1)*(X - s1)
# and a2*X^2 + b2*X + c2 = a2*(X - r2)*(X - s2)
# so that r1 + s1 = -b1/a1 and r1*s1 = c1/a1
# and r2 + s2 = -b2/a2 and r2*s2 = c2/a2,
#giving that mob1 is the same as:
tau :=
((a1*c2-a2*c1)*X + b1*c2-b2*c1)
/((a2*b1-a1*b2)*X + a2*c1-a1*c2);
#The follows gives 0,
#showing that mob1 and tau are the same:
check :=
mob1 -
```

```
subs(b1 = -(r1+s1)*a1, c1 = r1*s1*a1,
b2 = -(r2+s2)*a2, c2 = r2*s2*a2, tau);
simplify(\%);
#As another check, one can see
#that substituting X with tau changes
#each Fi to
#Resultant(F1,F2,X)*Fi/((a1*b2-a2*b1)*X+a1*c2-a2*c1)^2
factor(simplify(subs(X=tau, F1)));
factor(simplify(subs(X=tau, F2)));
#Now, give names to the
#numerator and denominator of tau:
numertau := (a1*c2-a2*c1)*X + b1*c2-b2*c1;
denomtau := (a2*b1-a1*b2)*X + a2*c1-a1*c2;
#So, this is the tau that swaps
#the roots of F1 and swaps the roots of F2.
#Now, the starting Y^2 = F0*F1*F2
#is reducible, which means that
#F0 is linearly dependent on F1, F2.
#That is, F0 = k1*F1 + k2*F2,
#for some k1,k2, which must be conjugate.
F0 := a0*X^2 + b0*X + c0;
#Note also that the same tau
#which swaps the roots of F1 and
#swaps the roots of F2 is also
#guaranteed to swap the roots of F0.
#We can also see in general what sigma looks like.
F0 := k1*F1 + k2*F2;
with(linalg);
Mtau
:= matrix
([[ coeff(numertau,X,1), coeff(numertau,X,0) ],
[ coeff(denomtau,X,1), coeff(denomtau,X,0) ]] );
MtauEvals :=
```

```
[eigenvals(transpose(Mtau))];
eval1 := MtauEvals[1];
eval2 := MtauEvals[2];
#But it's easy to see that these
#are just +- sqrt(ResF1F2):
#[N.B. also that resultant(F1,F2,X)
#is guaranteed to be in Q,
#even when F1,F2 are quadratic and
#conjugate, so that the eigenvalues
#are at worst quadratic.
eval1alt := sqrt(resultant(F1,F2,X));
eval2alt := -sqrt(resultant(F1,F2,X));
check := eval1 - eval1alt;
check := eval2 - eval2alt;
# Now, find the eigenvectors:
MtauEvects :=
[eigenvectors(transpose(Mtau))];
evect1 := MtauEvects[1][3][1];
# evector for eval sqrt(resultant(F1,F2,X))
evect2 := MtauEvects[2][3][1];
#evector for eval -sqrt(resultant(F1,F2,X))
#One might as well multiply
#the vectors through by (a1*b2-a2*b1):
evect1alt :=
[a1*b2 - a2*b1, a1*c2 - a2*c1 - sqrt(resultant(F1,F2,X))];
evect2alt :=
[a1*b2 - a2*b1, a1*c2 - a2*c1 + sqrt(resultant(F1,F2,X))];
#The following checks they are the same (up to scalars):
check:=
simplify( evect1alt[1]*evect1[2]
- evect1alt[2]*evect1[1] );
check :=
simplify( evect2alt[1]*evect2[2]
```

```
- evect2alt[2]*evect2[1] );
# This allows us to obtain the
# mobius transformation sigma, which is
# negated by tau:
sigma :=
( evect1alt[1]*X + evect1alt[2] )
/ ( evect2alt[1]*X + evect2alt[2] );
# ... that is to say:
sigma :=
( (a1*b2 - a2*b1)*X + a1*c2 -
a2*c1 - sqrt(resultant(F1,F2,X)) )/
( (a1*b2 - a2*b1)*X + a1*c2 -
a2*c1 + sqrt(resultant(F1,F2,X)) );
#The following gives 0, verifying
#that sigma is negated by tau:
check := simplify( sigma + subs(X=tau, sigma) );
# Of course, the above is
# degenerate if a1*b2 - a2*b1 = 0, since
# then the formulas don't give
# the two independent eigenvectors,
# due to the division by 0 in
# evect1, evect2. In this special
# case, should use either of the
# two following alternative formulas
# for the eigenvectors and for sigma:
# The following are o.k. as long
# as b1*c2-b2*c1 is nonzero:
# evect1altt := [a1*c2-a2*c1
# + sqrt(resultant(F1,F2,X)), b1*c2-b2*c1];
# evect2altt := [a1*c2-a2*c1
# - sqrt(resultant(F1,F2,X)), b1*c2-b2*c1];
# ssigma :=
# ( (a1*c2-a2*c1 + sqrt(resultant(F1,F2,X)))*X
```

```
# + b1*c2-b2*c1 )/
# ( (a1*c2-a2*c1 - sqrt(resultant(F1,F2,X)))*X
# + b1*c2-b2*c1 );
# For the very special case when i
# a1*b2 - a2*b1 = b1*c2-b2*c1 = 0,
# we must have b1 = b2 = 0
# (since otherwise F1 and F2 would be scalar
# multiples of each other, contradicting
# Y^2 = F0*F1*F2 being genus 2).
# In this special case, tau = -X
# and we can just take
# Mtau := [[1,0],[0,-1]] with
# evalues 1,-1 and evectors [1,0],[0,1],
# and sigma := X.
# Now, let's see what is
# the field of definition of sigma.
# It is certainly defined over the
# quartic field Q(sqrt(d),sqrt(ResF1F2)),
# where F1,F2 are defined over Q(sqrt(d))
# and ResF1F2 = resultant(F1,F2,x).
# Note that the combined action:
# sqrt(d) |-> -sqrt(d),
# sqrt(ResF1F2) |-> -sqrt(ResF1F2)
# swaps F1,F2, negates the
# numerator and denominator of sigma,
# and so leaves sigma unchanged.
# Therefore, sigma is in fact defined
# over the quadratic number field
# Q(sqrt(ResF1F2*d)).
ResF1F2 := resultant(F1,F2,X);
# Now, compute the inverse of sigma:
sigmainv
:= ( evect2alt[2]*T-evect1alt[2] )/
```

```
   ( -evect2alt[1]*T+evect1alt[1] );
  # ... that is to say:
sigmainv
:= -((a1*c2 - a2*c1)*(T-1)
+ sqrt(ResF1F2)*(T+1) )/
( (a1*b2 - a2*b1)*(T-1) );
# Check that is really is the inverse of sigma:
check:=simplify( subs( T = sigma, sigmainv ) );
#Now, change variable to T, with
# the map X |--> sigma(X) = T,
# by substituting X = sigmainv(T),
# and see what happens to each
# of F0,F1,F2 (we should find that only
# even powers of T occur modulo
# squares in the denominators, which
# can be incorporated into the y-coord):
F1T := subs( X = sigmainv, F1 );
# which is the same as:
#(2*a1*ResF1F2*(T^2 + 1) +
#(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2)*
#sqrt(ResF1F2)*(T^2 - 1))
#/( (a1*b2-a2*b1)^2*(T-1)^2 )
F1Tvar := (2*a1*ResF1F2*(T^2 + 1) +
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2)
*sqrt(ResF1F2)*(T^2 - 1))
/((a1*b2-a2*b1)^2*(T-1)^2 );
#Check they are the same:
check := simplify(F1T - F1Tvar);
#Similarly for F2:
F2T := subs( X = sigmainv, F2 );
# which is the same as:
F2Tvar := (2*a2*ResF1F2*(T^2 + 1) +
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)
```

```
*sqrt(ResF1F2)*(T^2 - 1))
/( (a1*b2-a2*b1)^2*(T-1)^2 );
# Check they are the same:
check := simplify(F2T - F2Tvar);
# ... and of course, F0T is just
# k1*F1T + k2*F2T, which also has
# only even powers of T. Then the map:
# (X,Y) |--> (T,y) =
# (sigma(X), Y*(a1*b2-a2*b1)^3*(T-1)^3 )
# transforms the original Y^2 = F0*F1*F2
# to y^2 = numer(F0T*F1T*F2T).
# Now, replacing T^2 by x,
# with x = sqrt(T), we get the
# result of the mapping
# (X,Y) |-> (x,y)
# = (sigma(X)^2, Y*sqrt(ResF1F2)*
# (a1*b2-a2*b1)^3*(sigma(X)-1)^3 )
# to the an elliptic curve
# Ea : y^2 = ResF1F2*F0xNumer*F1xNumer*F2xNumer,
# where:
F1xNumer := subs(T = sqrt(x), numer(F1Tvar));
F2xNumer := subs(T = sqrt(x), numer(F2Tvar));
F0xNumer := k1*F1x + k2*F2x;
# [similarly for Eb, on taking conjugates]
# ... that is to say:
F1xNumervar := (2*a1*ResF1F2*(x + 1) +
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2)
*sqrt(ResF1F2)*(x - 1));
F2xNumervar := 2*a2*ResF1F2*(x + 1) +
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)
*sqrt(ResF1F2)*(x - 1);
# Check they are the same:
F0xNumervar := k1*F1xNumervar + k2*F2xNumervar;
```

```
check := simplify( F1xNumer - F1xNumervar);
check := simplify( F2xNumer - F2xNumervar);
# So, Ea (and its conjugate Eb)
# can be both defined over Q(sqrt(d))
# and we can check here that the map
# (X,Y) |-> (x,y)
# = (sigma(X)^2, Y*sqrt(ResF1F2)*
# (a1*b2-a2*b1)^3*(sigma(X)-1)^3 )
# from Y^2 = F0*F1*F2 to
# Ea : y^2 =
# ResF1F2*F0xNumervar*F1xNumervar*F2xNumervar
# is as claimed above:
factor(subs(x=sigma^2,
y=Y*sqrt(ResF1F2)*(a1*b2-a2*b1)^3*
(sigma-1)^3,y^2))
- factor(subs(x=sigma^2,y =Y*sqrt(ResF1F2)
*(a1*b2-a2*b1)^3*(sigma-1)^3,
ResF1F2*F0xNumervar*F1xNumervar*F2xNumervar));
simplify( subs(Y^2=F0*F1*F2, factor(\%)) );
# Of course, the other curve Eb is just:
# Eb : bary^2 =
# ResF1F2*barF0xNumervar*barF1xNumervar*barF2xNumervar
# where barF0xNumervar, barF1xNumervar,
# barF2xNumervar are just the "flips"
# obtained by reversing the
# order of the coefficients (i.e. replacing
# x by 1/barx and multiplying through
# by a power of barx):
barF1xNumervar := (2*a1*ResF1F2*(1 + barx) +
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2)
*sqrt(ResF1F2)*(1 - barx));
barF2xNumervar := 2*a2*ResF1F2*(1 + barx) +
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)
```

```
*sqrt(ResF1F2)*(1 - barx);
barF0xNumervar
:= k1*barF1xNumervar + k2*barF2xNumervar;
# The flip is achieved by barx = 1/x and
# bary = y/sigma^3, so that the map
# (X,Y) |-> (barx,bary)
# = (1/sigma(X)^2, Y*sqrt(ResF1F2)*
# (a1*b2-a2*b1)^3*(sigma(X)-1)^3/sigma^3)
# is from Y^2 = F0*F1*F2 to
# Eb : bary^2 = ResF1F2*barF0xNumervar*
# barF1xNumervar*barF2xNumervar
# which we check as follows:
factor(subs(barx=1/sigma^2,
bary=Y*sqrt(ResF1F2)*(a1*b2-a2*b1)^3*
(sigma-1)^3/sigma^3,bary^2))
-factor(subs(barx=1/sigma^2,
bary =Y*sqrt(ResF1F2)*(a1*b2-a2*b1)^3*
(sigma-1)^3/sigma^3,
ResF1F2*barF0xNumervar*barF1xNumervar*
barF2xNumervar));
simplify( subs(Y^2=F0*F1*F2, factor(\%)) );

# It will be nice soon to have
# an x-coordinate defined over Q.
# At the moment, the map X |->
# sigma(X)^2 = x is defined over
# the quadratic field Q(sqrt(ResF1F2*d)).
# The numerator and denominator
# of sigma^2 are conjugates,
# so we can make mobius-transform to
# a Q-rational variable v by
# v = sqrt(ResF1F2*d)*(x + 1)/(x - 1),
# which has inverse
```

```
# x = (v + sqrt(ResF1F2*d))/(v - sqrt(ResF1F2*d)).
# Now, for the first part of the
# process, we have 3 genus 0 curves:
# EE0 : square = alpha0*F1*F2,
# EE1 : square = alpha1*F0*F2,
# EE2 : square = alpha2*F0*F1,
# where alpha0 is in Q, and
# alpha1, alpha2 are in Q(sqrt(d)) and conjugate.
# EE0 is defined over Q.
# EE1,EE2 are conjugate and we want first to
# map these to elliptic curves via a map which is Q-rational
# on the x-coordinates. We just do the simplest case where
# the alpha's are all 1
# (corresponding to the identity in J(Q)/phi(A(Q))).
# So, let v = sqrt(ResF1F2*d)*(x + 1)/(x - 1), as above,
# with inverse
# x = (v + sqrt(ResF1F2*d))/(v - sqrt(ResF1F2*d)).
# One could, at this stage, perform:
# subs(x=(v + sqrt(ResF1F2*d))
# /(v - sqrt(ResF1F2*d)),F1x) to get F1v,
# but one can actually immediately see F1v as follows.
# Note that the numer of F1T
# can have a factor of (T^2-1)*sqrt(ResF1F2)
# taken to the outside, and then
# numer and denom of F1T can be multiplied by
# sqrt(d) to give:
# (T^2 - 1)*sqrt(ResF1F2)*(2*a1*sqrt(d)*
# sqrt(ResF1F2)*(T^2 + 1)/(T^2 - 1) +
# sqrt(d)*(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# /( sqrt(d)*(a1*b2-a2*b1)^2*(T-1)^2 )
# Since v = sqrt(d)*sqrt(ResF1F2)*
# (T^2 + 1)/(T^2 - 1), this becomes:
```

```
F1v := (T^2 - 1)*sqrt(ResF1F2)*(2*a1*v +
sqrt(d)*(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
/( sqrt(d)*(a1*b2-a2*b1)^2*(T-1)^2 );
# Check they are the same:
check := simplify( F1T - subs
(v = sqrt(ResF1F2)*sqrt(d)*(T^2 + 1)/(T^2 - 1),
F1v) );
# Similarly for F2:
F2v := (T^2 - 1)*sqrt(ResF1F2)*(2*a2*v +
sqrt(d)*(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1))
/( sqrt(d)*(a1*b2-a2*b1)^2*(T-1)^2 );
# Check they are the same:
check := simplify( F2T - subs
(v = sqrt(ResF1F2)*sqrt(d)*(T^2 + 1)/(T^2 - 1),
F2v) );
F0v := k1*F1v + k2*F2v;
# Now, we do the map on EE1 : Y^2 = F0*F2.
# On inspecting
# Y^2 = F0v*F2v, we see that:
# (Y*d*(a1*b2-a2*b1)^2*(T-1)^2/(T^2-1))^2 =
# d*ResF1F2*(k1*(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# +k2*(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
# *(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1))
# If we wish, we can take sqrt(d)
# to be any expression that
# is negated by conjugation,
# such as sqrt(d) = 1/(b1*c2 - b2*c1).
# or even sqrt(d) =
# k1 - k2, for example.
# At this point, we can turn
```

```
# this into an elliptic curve
# by multiplying both sides by
# T^2 = x and incorporating the T^2
# on the LHS into the y-coordinate:
# (T*Y*d*(a1*b2-a2*b1)^2*(T-1)^2/(T^2-1))^2 =
# d*ResF1F2*x*(k1*(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# +k2*(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
# *(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1))
#  = d*ResF1F2*
# (v + sqrt(ResF1F2*d))/(v - sqrt(ResF1F2*d))
# *(k1*(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# +k2*(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
# *(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1))
# so that, on multiplying both
# sides by (v - sqrt(ResF1F2*d))^2:
# (T*Y*d*(v - sqrt(ResF1F2*d))*
# (a1*b2-a2*b1)^2*(T-1)^2/(T^2-1))^2 =
# d*ResF1F2*(v^2 - ResF1F2*d)
# *(k1*(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# +k2*(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
# *(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1))
# and cancelling (T-1) we get:
# (T*Y*d*(v - sqrt(ResF1F2*d))*
# (a1*b2-a2*b1)^2*(T-1)/(T+1))^2 =
```

```
# d*ResF1F2*(v^2 - ResF1F2*d)
# *(k1*(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# +k2*(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
# *(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1))
# and replacing
# v = sqrt(ResF1F2)*sqrt(d)*(T^2 + 1)/(T^2 - 1)
# gives:
# (T*Y*d*((T^2+1)/(T^2-1) - 1)*
# (a1*b2-a2*b1)^2*(T-1)/(T+1))^2 =
# (v^2 - ResF1F2*d)
# *(k1*(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# +k2*(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
# *(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1))
# and so:
# (2*T*Y*d*(a1*b2-a2*b1)^2/(T+1)^2)^2 =
# (v^2 - ResF1F2*d)
# *(k1*(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# +k2*(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
# *(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1))
# [note, it's easy to check that
# the Y-coord map is defined over Q]
# The map can be checked with:
(2*T*Y*d*(a1*b2-a2*b1)^2/(T+1)^2)^2 -
(v^2 - ResF1F2*d)
```

```
*(k1*(2*a1*v + sqrt(d)*
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
+k2*(2*a2*v + sqrt(d)*
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
*(2*a2*v + sqrt(d)*
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1));
subs(T=sigma,subs
(v=sqrt(ResF1F2)*sqrt(d)*(T^2 + 1)/(T^2 - 1),\%));
simplify( subs( Y^2 = F0*F2, factor(\%) ) );
# In summary, we have established a map:
# (X,Y) |-> (v,y), where:
# v = sqrt(ResF1F2)*sqrt(d)*(sigma^2 + 1)/(sigma^2 - 1)
# y = 2*sigma*Y*d*(a1*b2-a2*b1)^2/(sigma+1)^2
# (both of which are easily
# checked to be defined over Q)
# which is from our genus 1 curve EE1 : Y^2 = F0*F2
# to the elliptic curve: y^2 = Qv*L0v*L2v, where:
Qv := (v^2 - ResF1F2*d);
L0v := k1*(2*a1*v + sqrt(d)*
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
+k2*(2*a2*v + sqrt(d)*
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1));
L2v := 2*a2*v + sqrt(d)*
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1);
# and note that the quadratic Qv is defined over Q,
# the linear L0v is defined over Q and
# the linear L2v is defined over Q(sqrt(d)).
# It is still in quartic form,
# but we can find the root of L0v:
v0 := solve(L0v,v);
# which gives the result:
# v0 := 1/2*d^(1/2)*
# (2*k1*a1*a2*c1-2*k1*a1^2*c2-k1*a2*b1^2+k1*b1*a1*b2
```

```
# -k2*b2*a2*b1-2*k2*a2*a1*c2+k2*a1*b2^2+2*c1*k2*a2^2)
# /(k1*a1+k2*a2);
factor(subs(v = v0 + 1/u, v^2 - ResF1F2*d));
# gave the result:
# ( d*(a1*b2-a2*b1)^2*
# (k2^2*b2^2+2*k1*b1*k2*b2-4*a1*c1*k1^2
# -4*a1*k1*c2*k2-4*k2^2*a2*c2+k1^2*b1^2-4*c1*k1*k2*a2)
# *u^2
# +4*d^(1/2)*(k1*a1+k2*a2)*
# (2*k1*a1*a2*c1-2*k1*a1^2*c2-k1*a2*b1^2
# +k1*b1*a1*b2-k2*b2*a2*b1-2*k2*a2*a1*c2+
# k2*a1*b2^2+2*c1*k2*a2^2)*u
# +4*(k1*a1+k2*a2)^2 )/
# ( 4*(k1*a1+k2*a2)^2*u^2 );
check := factor
(subs(v = v0 + 1/u, v^2 - ResF1F2*d)) -
(d*(a1*b2-a2*b1)^2*
(k2^2*b2^2+2*k1*b1*k2*b2-4*a1*c1*k1^2
-4*a1*k1*c2*k2-4*k2^2*a2*c2+
k1^2*b1^2-4*c1*k1*k2*a2)*u^2
+4*d^(1/2)*(k1*a1+k2*a2)*
(2*k1*a1*a2*c1-2*k1*a1^2*c2-k1*a2*b1^2
+k1*b1*a1*b2-k2*b2*a2*b1-2*k2*a2*a1*c2+
k2*a1*b2^2+2*c1*k2*a2^2)*u
+4*(k1*a1+k2*a2)^2 )
/(4*(k1*a1+k2*a2)^2*u^2 );
simplify(\%);
factor(subs(v = v0 + 1/u, L0v));
# gave the result: 2*(k1*a1+k2*a2)/u
check :=
factor(subs(v = v0 + 1/u, L0v)) - 2*(k1*a1+k2*a2)/u;
simplify(\%);
factor(subs(v = v0 + 1/u, L2v));
```

```
# gave the result:
# ( -d^(1/2)*k1*(a1*b2-a2*b1)^2*u
# + 2*a2*(k1*a1+k2*a2) )/( (k1*a1+k2*a2)*u );
check
:= factor(subs(v = v0 + 1/u, L2v)) -
( -d^(1/2)*k1*(a1*b2-a2*b1)^2*u
+ 2*a2*(k1*a1+k2*a2) )/( (k1*a1+k2*a2)*u );
simplify(\%);
# On absorbing the denominators in y^2, we get:
# yy^2 = Qu*L2u, where:
yy := 2*y*(k1*a1+k2*a2)/(v-v0)^2;
# same as 2*y*(k1*a1+k2*a2)*u^2
Qu := d*(a1*b2-a2*b1)^2*
(k2^2*b2^2+2*k1*b1*k2*b2-4*a1*c1*k1^2
-4*a1*k1*c2*k2-4*k2^2*a2*c2+k1^2*b1^2
-4*c1*k1*k2*a2)*u^2
+4*d^(1/2)*(k1*a1+k2*a2)*
(2*k1*a1*a2*c1-2*k1*a1^2*c2-k1*a2*b1^2
+k1*b1*a1*b2-k2*b2*a2*b1-
2*k2*a2*a1*c2+k2*a1*b2^2+2*c1*k2*a2^2)*u
+4*(k1*a1+k2*a2)^2;
L2u := -2*d^(1/2)*k1*(a1*b2-a2*b1)^2*u
+ 4*a2*(k1*a1+k2*a2);
check := yy^2 - subs(u = 1/(v-v0), Qu*L2u);
subs(y^2 = Qv*L0v*L2v, \%);
simplify(\%);
# So, the curve
# yy^2 = Qu*L2u is our required form.
# To be systematic, it is probably
# better always to use the above
# map to obtain the quadratic-over-Q
# and the linear-over-Q(sqrt(d))
# for the next step, and avoid
```

```
# ways of getting a quadratic and linear
# (even when other maps are possible).
# Similarly from EE2 : Y^2 = F0*F1, we get:
# (2*T*Y*d*(a1*b2-a2*b1)^2/(T+1)^2)^2 =
# (v^2 - ResF1F2*d)
# *(k1*(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# +k2*(2*a2*v + sqrt(d)*
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
# *(2*a1*v + sqrt(d)*
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
# The map can be checked with:
(2*T*Y*d*(a1*b2-a2*b1)^2/(T+1)^2)^2 -
(v^2 - ResF1F2*d)
*(k1*(2*a1*v + sqrt(d)*
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
+k2*(2*a2*v + sqrt(d)*
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)))
*(2*a1*v + sqrt(d)*
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2));
subs(T=sigma,subs(v=sqrt(ResF1F2)*sqrt(d)
*(T^2 + 1)/(T^2 - 1),\%));
simplify( subs( Y^2 = F0*F1, factor(\%) ) );
# In summary, we have established a map
# [the same map as for EE1]:
# (X,Y) |-> (v,y), where:
# v = sqrt(ResF1F2)*sqrt(d)*(sigma^2 + 1)/(sigma^2 - 1)
# y = 2*sigma*Y*d*(a1*b2-a2*b1)^2/(sigma+1)^2
# (both of which are easily checked
# to be defined over Q)
# which is from our genus 1 curve
# EE2 : Y^2 = F0*F1
# to the elliptic curve:
```

```
# y^2 = Qv*L0v*L1v, where:
Qv := (v^2 - ResF1F2*d);
L0v :=
k1*(2*a1*v + sqrt(d)*
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2))
+k2*(2*a2*v + sqrt(d)*
(-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1));
L1v :=
2*a1*v + sqrt(d)*
(-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2);
# and note again that the
# quadratic Qv is defined over Q,
# the linear L0v is defined over Q and
# the linear L1v is defined over Q(sqrt(d)).
# Taking v0 to be the root of
# L0v and u = 1/(v-v0) (as before), we get:
# E2 : yy^2 = Qu*L1u, where:
yy := 2*y*(k1*a1+k2*a2)/(v-v0)^2;
# same as 2*y*(k1*a1+k2*a2)*u^2
Qu :=
d*(a1*b2-a2*b1)^2*
(k2^2*b2^2+2*k1*b1*k2*b2-4*a1*c1*k1^2
-4*a1*k1*c2*k2-4*k2^2*a2*c2+k1^2*
b1^2-4*c1*k1*k2*a2)*u^2
+4*d^(1/2)*(k1*a1+k2*a2)*
(2*k1*a1*a2*c1-2*k1*a1^2*c2-k1*a2*b1^2
+k1*b1*a1*b2-k2*b2*a2*b1-2*k2*a2*a1*c2
+k2*a1*b2^2+2*c1*k2*a2^2)*u
+4*(k1*a1+k2*a2)^2;
L1u :=
2*d^(1/2)*k2*(a1*b2-a2*b1)^2*u
+4*a1*(k1*a1+k2*a2);
# [same as L1u, except with
```

```
# each ?1 swapped with ?2
# and sqrt(d) replaced by -sqrt(d)]

check := yy^2 - subs(u = 1/(v-v0), Qu*L1u);
subs(y^2 = Qv*L0v*L1v, \%);
simplify(factor(\%));

# In summary, we have taken our
# genus 1 curves (in quartic form):
# EE1: Y^2 = F0*F2 and EE2: Y^2 = F0*F1
# and used (X,Y) |--> (u,yy)
# [both u and yy defined over Q] above
# to map to: E1 : yy^2 = Qu*L2u
# and E2 : yy^2 = Qu*L1u,
# where Qu is a quadratic defined over Q,
# and L1u,L2u are either
# both defined over Q,
# or are quadratic and conjugate.
# Note that these are 2-to-1 maps
# (not birational transformations)
# which presumably induce
# isogenies on the Jacobians.
# It is also worth mentioning
# the special case when sigma is
# already defined over Q.
# This happens when d*ResF1F2 is square
# (an example is F1 = X^2 + I*p
# and F2 = X^2 - I*p, when
# d = -1 and ResF1F2 = -4*p^2).
# In this case, T = sigma
# is already defined over Q. Recall:
# F1Tvar := (2*a1*ResF1F2*(T^2 + 1) +
# (-2*a1*a2*c1+2*a1^2*c2+a2*b1^2-b1*a1*b2)
```

```
# *sqrt(ResF1F2)*(T^2 - 1))
# /((a1*b2-a2*b1)^2*(T-1)^2 );
# F2Tvar := (2*a2*ResF1F2*(T^2 + 1) +
# (-2*a2^2*c1+2*a2*a1*c2-a1*b2^2+b2*a2*b1)
# *sqrt(ResF1F2)*(T^2 - 1))
# /((a1*b2-a2*b1)^2*(T-1)^2 );
# F0Tvar := k1*F1Tvar + k2*F2Tvar;
# so that EE1 : Y^2 = F0*F2 gives:
# (Y*(a1*b2-a2*b1)^2*(T-1)^2)^2
# = x*F0xNumer*F2xNumer;
# where F0xNumer
# := k1*F1xNumer + k2*F2xNumer;
# Similarly EE2 : Y^2 = F0*F1 gives:
# (Y*(a1*b2-a2*b1)^2*(T-1)^2)^2
# = x*F1xNumer*F2xNumer;
# The map (X,Y) |->
# (x,Y*(a1*b2-a2*b1)^2*(T-1)^2) is (for
# this special case) already
# defined over Q, and the resulting
# curves are already of the required
# form, without needing
# to use v (although it doesn't do any harm).
# Note that, for consistency we should
# probably still map
# the root of F1xNumer to infinity.

# For the next step, we start with:
# E1 : yy^2 = Qu*L2u,
# where Qu is quadratic and
# defined over Q, and L2u is linear
# and defined over Q(sqrt(d)).
# Say, L2u = L2rat + L2sqrtd*sqrt(d),
# where L2rat, L2sqrtd are both defined over Q.
```

```
Qu := a*u^2 + b*u + c;
L2rat := g2*u + h2;
L2sqrtd := i2*u + j2;
# so that:
L2u := L2rat + L2sqrtd*sqrt(d);

# Now, let yy = r + s*sqrt(d), so that:
# (r + s*sqrt(d))^2 = Qu*(L2rat + L2sqrtd*sqrt(d));
E1:=
(r + s*sqrt(d))^2 - Qu*(L2rat + L2sqrtd*sqrt(d));
# so that our elliptic curve is E1 = 0.
E1 := expand(E1);
# Now split E1 into its
# rational part and coeff of sqrt(d):
E1sqrtd := coeff(E1, sqrt(d));
# which corresponds to: 2*r*s - Qu*L2sqrtd
# that is, the equation: 2*r*s = Qu*L2sqrtd.
E1rat := expand(E1 - sqrt(d)*E1sqrtd);
# which corresponds to: r^2 + d*s^2 - Qu*L2rat
# that is, the equation: r^2 + d*s^2 = Qu*L2rat
# Now, use the first equation to solve for r:
solve(E1sqrtd,r);
# and substitute into the second equation:
eqna := subs(r=\%, E1rat);
# which gives:
# Qu^2*L2sqrtd^2/(4*s^2) + d*s^2 = Qu*L2rat
# eqna := Qu^2*L2sqrtd^2/(4*s^2)
# + d*s^2 - Qu*L2rat;
# Now let t = s^2/Qu:
eqnb := simplify(4*t*subs(s = sqrt(t*Qu), eqna)/Qu);
# which is the same as:
# L2sqrtd^2 + 4*d*t^2 = 4*L2rat*t
```

```
# eqnb := L2sqrtd^2 + 4*d*t^2 - 4*L2rat*t;
# We want to parametrise the genus 0
# curve eqnb as t(z),u(z).
# Rather than just letting Maple
# choose some random parametrisation,
# it's better to fix a natural
# choice of basepoint, such
# as u = root of L2sqrtd,
# t = 0, which satisfies eqnb.
eqnc := simplify(subs(t = L2sqrtd*z, eqnb)/L2sqrtd);
# which is the same as:
# L2sqrtd + 4*d*L2sqrtd*z^2 = 4*L2rat*z
# eqnc := L2sqrtd + 4*d*L2sqrtd*z^2 - 4*L2rat*z;
uz := solve(eqnc, u);
# which gives:
uz := -(j2+4*z^2*d*j2-4*z*h2)/(i2+4*i2*z^2*d-4*z*g2);
tz := simplify(subs(u=uz, L2sqrtd*z));
# which gives:
tz := 4*z^2*(h2*i2-g2*j2)/(i2+4*i2*z^2*d-4*z*g2);
# Check that this is a parametrisation of eqnb:
check := simplify(subs(u=uz, t=tz, eqnb));
# Our new genus 2 curve is then s^2 = tz*Qu(uz);
Quz := factor(simplify(subs(u=uz, Qu)));
# which gives:
Quz :=
(a*j2^2+8*a*z^2*d*j2^2-8*a*z*h2*j2+
16*a*z^4*d^2*j2^2-32*a*z^3*d*j2*h2+16*a*z^2
*h2^2-b*i2*j2-8*b*z^2*d*i2*j2+4*b*z*g2*j2
-16*b*z^4*d^2*j2*i2+16*b*z^3*d*j2*g2+
4*b*z*h2*i2+16*b*z^3*h2*i2*d-16*b*z^2*h2*g2
+c*i2^2+8*c*z^2*d*i2^2-8*c*z*g2*i2+
16*c*i2^2*z^4*d^2-32*c*i2*z^3*d*g2+16*c*z^2*g2^2)
/(i2+4*i2*z^2*d-4*z*g2)^2;
```

```
# so that s^2 = tz*Quz becomes:
# ss^2 = ttz*QQuz, where:
ss := s*(i2+4*i2*z^2*d-4*z*g2)^2/(2*z);
ttz := (h2*i2-g2*j2)*(i2+4*i2*z^2*d-4*z*g2);
QQuz :=
a*j2^2+8*a*z^2*d*j2^2-8*a*z*h2*j2+
16*a*z^4*d^2*j2^2-32*a*z^3*d*j2*h2+16*a*z^2
*h2^2-b*i2*j2-8*b*z^2*d*i2*j2+4*b*z*g2*j2
-16*b*z^4*d^2*j2*i2+16*b*z^3*d*j2*g2+
4*b*z*h2*i2+16*b*z^3*h2*i2*
(-16)*b*z^2*h2*g2+c*i2^2+8*c*z^2*d*i2^2-8*c*z*g2*i2+
16*c*i2^2*z^4*d^2-32*c*i2*z^3*d*g2+16*c*z^2*g2^2;
check := subs(s^2 = tz*Quz, ss^2 - ttz*QQuz);
# So, ss^2 = ttz*QQuz is our new genus 2 curve over Q,
# where ttz is quadratic and QQuz is quartic.
# Note also that Qu has roots:
# 1/2/a*(-b+(b^2-4*a*c)^(1/2)),
# 1/2/a*(-b-(b^2-4*a*c)^(1/2))
# and so 4*a*Qu is just:
# (2*a*u + b + (b^2-4*a*c)^(1/2))
# *(2*a*u + b - (b^2-4*a*c)^(1/2))
# Now, note that:
G1 := subs(u=uz, 2*a*u + b +
(b^2-4*a*c)^(1/2))*(i2+4*i2*z^2*d-4*z*g2);
# which is the same as:
G1 := -2*a*j2-8*a*z^2*d*j2+8*a*z*h2+
b*i2+4*b*i2*z^2*d-4*b*z*g2
+(i2+4*i2*z^2*d-4*z*g2)*(b^2-4*a*c)^(1/2);
# Similarly:
G2 := subs(u=uz, 2*a*u + b -
(b^2-4*a*c)^(1/2))*(i2+4*i2*z^2*d-4*z*g2);
# which is the same as:
G2 := -2*a*j2-8*a*z^2*d*j2+8*a*z*h2+
```

```
b*i2+4*b*i2*z^2*d-4*b*z*g2
-(i2+4*i2*z^2*d-4*z*g2)*(b^2-4*a*c)^(1/2);
# Also, absorb a factor of "a" into ttz and call it G0:
G0 := a*ttz;
# which is the same as:
G0 := a*(h2*i2-g2*j2)
*(i2+4*i2*z^2*d-4*z*g2);
# Note that G0*G1*G2 = 4*a^2*ttz*QQuz
check := factor
(simplify(expand(G0*G1*G2))) - 4*a^2*ttz*QQuz;
# so that the genus 2 curve
# ss^2 = ttz*QQuz can be written as
# sss^2 = G0*G1*G2, where
# sss = 2*a*ss = s*a*(i2+4*i2*z^2*d-4*z*g2)^2/z;
sss := s*a*(i2+4*i2*z^2*d-4*z*g2)^2/z;
# Simlarly:
G2 := subs(u=uz, 2*a*u + b -
(b^2-4*a*c)^(1/2))*(i2+4*i2*z^2*d-4*z*g2);
# which is the same as:
G2 := -2*a*j2-8*a*z^2*d*j2+8*a*z*h2+
b*i2+4*b*i2*z^2*d-4*b*z*g2
-(i2+4*i2*z^2*d-4*z*g2)*(b^2-4*a*c)^(1/2);
# Also, absorb a factor of "a" into ttz and call it G0:
G0 := a*ttz;
# which is the same as:
G0 := a*(h2*i2-g2*j2)*(i2+4*i2*z^2*d-4*z*g2);
# Note that G0*G1*G2 = 4*a^2*ttz*QQuz
check :=
factor(simplify(expand(G0*G1*G2))) - 4*a^2*ttz*QQuz;
# so that the genus 2 curve
# ss^2 = ttz*QQuz can be written as
# sss^2 = G0*G1*G2, where
# sss = 2*a*ss = s*a*(i2+4*i2*z^2*d-4*z*g2)^2/z;
```

```
sss := s*a*(i2+4*i2*z^2*d-4*z*g2)^2/z;
check := simplify(subs(s^2 = tz*Quz, sss^2 - G0*G1*G2));
# In summary, our genus 2 curve
# over Q is: sss^2 = G0*G1*G2,
# where G0,G1,G2 are at most
# quadratic, where G0 is defined over Q,
# and where G1,G2 are either defined over Q
# (which happens when Qu factors
# into linear factors over Q)
# or G1,G2 are defined over a quadratic
# number field and are conjugate
# (when Qu was irreducible).
# Note also that G0 is linearly
# dependent on G1,G2. Take:
kk1 := 1/2*a*(h2*i2-g2*j2)/(b^2-4*a*c)^(1/2);
kk2 := -1/2*a*(h2*i2-g2*j2)/(b^2-4*a*c)^(1/2);
# Then kk1 and kk2 are conjugates,
# and G0 = kk1*G1 + kk2*G2:
check := simplify(kk1*G1 + kk2*G2 - G0);
# So we are now through a
# complete cycle, and G0,G1,G2 can
# be taken as the F0,F1,F2 for a new cycle.
# Of course, if the same process
# were to be performed with
# the conjugate E2 : yy^2 = Qu*L1u,
# where L1u is the conjugate of L2u,
# then the final genus 2
# curve would be the same.
# It is worth mentioning here
# the exceptional case when d=1;
# that is to say, when L1u and
# L2u are defined over Q.
# In that case, it is not obvious,
```

```
# just by looking at L2u alone (say)
# how to write L2u as
# L2u := L2rat + L2sqrtd*sqrt(d).
# In that case you should use both
# L1u and L2u (from the previous step)
# and note that:
# L2u := L2rat + L2sqrtd*sqrt(d);
# L1u := L2rat - L2sqrtd*sqrt(d);
# so one can take, when d=1:
# L2rat := (L2u + L1u)/2;
# L2sqrtd := (L2u - L1u)/2;
# after which the algebra for getting
# G0,G1,G2 from E1 is the same as before.


# Might as well apply the above to an example.
# We have our starting curve
# Y^2 = (X^2 + p)*(X^2 - p*I)*(X^2 + p*I),
# so that:
F0 := X^2 + p;
F1 := X^2 - p*I;
F2 := X^2 + p*I;
a0 := coeff(F0,X,2);
b0 := coeff(F0,X,1);
c0 := coeff(F0,X,0);
a1 := coeff(F1,X,2);
b1 := coeff(F1,X,1);
c1 := coeff(F1,X,0);
a2 := coeff(F2,X,2);
b2 := coeff(F2,X,1);
c2 := coeff(F2,X,0);
ResF1F2 := resultant(F1,F2,X);
# which gave: -4*p^2
```

```
# Note that sqrt(ResF1F2)
# annoyingly gives 2*(-p^2)^(1/2) and
# we'd prefer p to be taken to the outside:
rr := factors(factor(resultant(F1,F2,X)));
sqrtResF1F2
:= sqrt(rr[1])*product(
(rr[2][i][1])^(iquo(rr[2][i][2],2))
*(sqrt(rr[2][i][1]))^(irem(rr[2][i][2],2)),
i = 1..nops(rr[2]));
# which gives the nicer form of the result:
sqrtResF1F2 := 2*I*p;
# We can solve for k1,k2
# using one of:
# k1 := (b2*a0-b0*a2)/(a1*b2-a2*b1);
# k2 := (-b1*a0+a1*b0)/(a1*b2-a2*b1);
# or, k1 := -(a2*c0-a0*c2)/(a1*c2-a2*c1);
# k2 := (a1*c0-c1*a0)/(a1*c2-a2*c1);
# or, k1 := (b2*c0-b0*c2)/(-b1*c2+b2*c1);
# k2 := -(b1*c0-c1*b0)/(-b1*c2+b2*c1);
# The first would involve
# division by 0, so use the second:
k1 := -(a2*c0-a0*c2)/(a1*c2-a2*c1);
k2 := (a1*c0-c1*a0)/(a1*c2-a2*c1);
k1 := expand(k1); k2 := expand(k2);
# This gave the result:
k1 := 1/2+1/2*I;
k2 := 1/2-1/2*I;
# Now check that indeed F0 := k1*F1 + k2*F2:
check := expand(k1*F1 + k2*F2 - F0);
# Of course, it is obvious that
# the involution which swaps the roots
# of G1 and swaps the roots of G2 is just X |-> -X,
# but we might as well test the formula in Lemma{lem:tau}:
```

```
tau := ((a1*c2-a2*c1)*X + b1*c2-b2*c1)
/((a2*b1-a1*b2)*X + a2*c1-a1*c2);
# and indeed it gives tau := -X, as expected.
# Also, sigma is the exceptional case where b1*c2-b2*c1 and
# a2*b1-a1*b2 are both 0, since b1=b2=0, when we have:
sigma := X;
sigmainv := T;
# Now, focus on the 3 curves relating to the identity:
# EE0 : Y^2 = F1*F2 = X^4 + p^2,
# EE1 : Y^2 = F0*F2 = (X^2 + p)*(X^2 + I*p),
# EE2 : Y^2 = F0*F1 = (X^2 + p)*(X^2 - I*p).
# The first of these is an elliptic curve over Q, isogenous
# under (X,Y) |-> (X^2, X*Y) to y^2 = x*(x^2 + p^2).
# It's rank is relevant (if the rank is 0, then the method is
# immediately successful in excluding this case), but is
# not need for constructing the next genus 2 curve
# (which only involves EE1,EE2). We first need to map EE1,EE2
# to elliptic curves E1,E2 of the form:
# square = (quadratic over Q)*(linear over Q(I)),
# and such that the map on the x-coordinate is Q-rational.
F0T := subs(X = sigmainv, F0);
F1T := subs(X = sigmainv, F1);
F2T := subs(X = sigmainv, F2);
# At this point, we have only even-power terms in T, and so
# EE1 : Y^2 = F0T*F2T = (T^2 + p)*(T^2 + I*p) becomes:
#       (T*Y)^2 = T^2*(T^2 + p)*(T^2 + I*p)
# and EE2 : Y^2 = F0T*F1T = (T^2 + p)*(T^2 - I*p) becomes:
#       (T*Y)^2 = T^2*(T^2 + p)*(T^2 - I*p)
F0x := subs(T = sqrt(x), F0T);
F1x := subs(T = sqrt(x), F1T);
F2x := subs(T = sqrt(x), F2T);
# ... which means that EE1 maps under (X,Y) |-> (X^2, X*Y) to:
# square = x*(x + p)*(x + I*p)
```

```
# and EE2 maps under the same
# map to: square = x*(x + p)*(x - I*p)
# These are already of the required form:
# (quadratic over Q)*(linear over Q(I)),
# and the map X |-> x = sigma^2 = X^2
# is already Q-rational.
# However, note that
# this example is unusual in that
# normally that map X |-> x = sigma^2
# is not Q-rational. We normally
# need a further mobius transformation
# to give v, which is Q-rational.
# It is worth (for being systematic)
# going through what the elliptic
# curves become if we stick strictly
# to the steps given above
# for the general case.
# These say that we should now
# change from x to v, where
# v := sqrt(d*ResF1F2)*(x+1)/(x-1),
# where d = -1 and ResF1F2 = -4*p^2,
# so that sqrt(d*ResF1F2) = 2*p,
# so that:
# v := 2*p*(x+1)/(x-1) which
# has inverse x := (v+2*p)/(v-2*p);
# We now see what:
# square = x*(x + p)*(x + I*p) becomes:
subs( x = (v+2*p)/(v-2*p),
x*(x + p)*(x + I*p) );
# We can multiply through by (v - 2*p)^4,
# which is square and so
# can be absorbed into y^2:
E1v := factor(\%*(v-2*p)^4);
```

```
# This gave the result:
# (v+2*p)*(v-2*p)*
# (v+v*p+2*p-2*p^2)*(v+2*p+I*p*v-2*I*p^2)
# where the linear factor
# v+v*p+2*p-2*p^2 arose from x + p,
# which in turn arose from
# F0 = X^2 + p. The general strategy
# tells us that we should first find
# v0, the root of this factor:
v0 := solve(v+v*p+2*p-2*p^2,v);
# and now we map to u = 1/(v-v0),
# with inverse v = v0 + 1/u,
# which has the effect of
# mapping (v0,0) to infinity:
factor( subs(v = v0 + 1/u, E1v) );
# We also multiply through by
# u^4*(p+1)^2, which gets absorbed into the y^2:
\%*u^4*(p+1)^2;
# .. and a linear change in
# u takes it to a nicer form:
factor( subs( u = ( -1/4*(p+1)^2/p^3 )*u
- 1/4*(p+1)/p^2, \% ) )*p^4/(p+1)^6;
# which gives: E1: square = u*(u+p)*( (1-I)*u - I*p )
# Similarly E2: square = u*(u+p)*( (1+I)*u + I*p )
# So for step 2 applied to E1,E2, we can either use:
# E1 : yy^2 = Qx*L2x = x*(x+p)*(x+I*p)
# E2 : yy^2 = Qx*L1x = x*(x+p)*(x-I*p)
# (as in the article) OR we could use the "systematic" choice:
# E1 : yy^2 = Qu*L2u = u*(u+p)*( (1-I)*u - I*p )
# E2 : yy^2 = Qu*L1u = u*(u+p)*( (1+I)*u + I*p )
# Since the two versions of E1
# are birat equiv (as are the two
# versions of E2), the resulting
```

```
# genus 2 curve should be the
# same (up to birat equiv)
# either way. Still, it doesn't do any
# harm to follow it through
# using both versions, just in case
# one version makes cycling
# easier to spot than the other.
# We are studying
# points (x,yy) on E1 with
# x in Q and yy in Q(sqrt(d)) = Q(I).
Qx := x*(x+p);
L2x := x+I*p;
d := -1;
L2rat := x;  # the rational part of L2x
L2sqrtd := p;
# the part of L2x being multiplied by sqrt(d) = I
# so that: L2x := L2rat + L2sqrtd*sqrt(d);
a := coeff(Qx,x,2);
b := coeff(Qx,x,1);
c := coeff(Qx,x,0);
# so that Qx := a*x^2 + b*x + c;
g2 := coeff(L2rat,x,1);
h2 := coeff(L2rat,x,0);
# so that L2rat := g2*x + h2;
i2 := coeff(L2sqrtd,x,1);
j2 := coeff(L2sqrtd,x,0);
# so that L2sqrtd := i2*x + j2;
# Now, let yy = r + s*sqrt(d), so that:
# (r + s*sqrt(d))^2
# = Qx*(L2rat + L2sqrtd*sqrt(d));
E1 := (r + s*sqrt(d))^2 -
Qx*(L2rat + L2sqrtd*sqrt(d));
# so that our elliptic curve is E1 = 0.
```

```
# For this example, this gives:
# E1 := (r+I*s)^2-x*(x+p)*(x-p)
E1 := expand(E1);
# Now split E1 into its
# rational part and coeff of sqrt(d):
E1sqrtd := coeff(E1, sqrt(d));
# which corresponds to:
# 2*r*s - Qx*L2sqrtd = 2*r*s-p*x^2-x*p^2
# that is, the equation:
# 2*r*s = Qx*L2sqrtd. i.e. 2*r*s = p*x^2+x*p^2
E1rat := expand(E1 - sqrt(d)*E1sqrtd);
# which corresponds to:
# r^2 + d*s^2 - Qx*L2rat = r^2-s^2-x^3-p*x^2
# that is, the equation:
# r^2 + d*s^2 = Qx*L2rat i.e. r^2-s^2 = x^3+p*x^2
# Now, use the first equation to solve for r:
solve(E1sqrtd,r); # which gives: 1/2*p*x*(x+p)/s
# and substitute into the second equation:
eqna := subs(r=\%, E1rat);
# which gives:
# Qx^2*L2sqrtd^2/(4*s^2) + d*s^2 = Qx*L2rat
# eqna := Qx^2*L2sqrtd^2/(4*s^2)
# + d*s^2 - Qx*L2rat;
# Now let t = s^2/Qx:
eqnb := simplify(4*t*subs
(s = sqrt(t*Qx), eqna)/Qx);
# which is the same as:
# L2sqrtd^2 + 4*d*t^2 = 4*L2rat*t
# eqnb
# := L2sqrtd^2 + 4*d*t^2 - 4*L2rat*t;
# In this example, this gives:
# p^2 - 4*t^2 - 4*t*x
# which is the equation:
```

```
# 4*t*x = -4*t^2 + p^2
# We want to parametrise the
# genus 0 curve eqnb as t(z),x(z).
# Rather than just letting Maple
# choose some random parametrisation,
# it's better to fix a natural
# choice of basepoint, such
# as x = root of L2sqrtd,
# t = 0, which satisfies eqnb.
eqnc :=
simplify(subs(t = L2sqrtd*z, eqnb)/L2sqrtd);
# which is the same as:
# L2sqrtd + 4*d*L2sqrtd*z^2 = 4*L2rat*z
# eqnc :=
# L2sqrtd + 4*d*L2sqrtd*z^2 - 4*L2rat*z;
# which in this case is:
# eqnc := p-4*z*x-4*p*z^2;
xz := solve(eqnc, x);
# which gives xz := -1/4*p*(-1+4*z^2)/z
# Of course, we could also have
# just used the general formula for xz
# xz := -(j2+4*z^2*d*j2-4*z*h2)
# /(i2+4*i2*z^2*d-4*z*g2);
# which gives the same answer.
tz := simplify(subs(x=xz, L2sqrtd*z));
# which gives: tz := p*z;
# Again, we could also have
# just used our general formula:
# tz := 4*z^2*(h2*i2-g2*j2)
# /(i2+4*i2*z^2*d-4*z*g2);
# which gives the same answer.
# Check that this is a
# parametrisation of eqnb:
```

```
check := simplify(subs(x=xz, t=tz, eqnb));
# Our new genus 2 curve is then s^2 = tz*Qx(xz);
# factor(simplify(tz*subs(x=xz, Qx)));
# In fact, the model is slightly
# simpler with a linear adjustment
# of z, and absorbing
# 64*(z+2*p)^2 into the s^2:
64*(z+2*p)^2*factor
(subs(z= z/(4*p) + 1/2, tz*subs(x=xz, Qx)));
# which gives the result:
# z*(z + 2*p)*(z + 4*p)*(z^2 - 8*p^2),
# We should keep track of
# where the different factors come from:
# We should take as G0
# (our new F0) to be the factor coming from tz:
G0 := 4*factor(subs(z= z/(4*p) + 1/2, tz));
# which gives: G0 := z+2*p;
# Now, recall that our original
# Qx factors as: x*(x+p) [of course,
# for a typical example,
# Qx will factor over a quadratic field extension].
# G1 and G2 (our new F1 and F2)
# are what arise from these factors x and x+p:
G1 := 4*(z+2*p)^2*
factor(subs(z= z/(4*p) + 1/2, subs(x=xz,x)));
# which gives: G1 := -z*(z+2*p)*(z+4*p);
# But note that
# z*(z+2*p)*(z+4*p)*(z^2-8*p^2) = square, and
# so G1 = -z*(z+2*p)*(z+4*p)
# = -(z^2-8*p^2) modulo squares.
# Up to a constant:
G1 := z^2-8*p^2;
# Also:
```

```
G2 := 4*(z+2*p)^2*
factor(subs(z= z/(4*p) + 1/2, subs(x=xz,x+p)));
# which gives: G2 := -(z+2*p)*(z^2 - 8*p^2);
# which mod squares
# and up to a constant is just:
G2 := z*(z+4*p);
# So, this is a complete cycle,
# and we can take our new F0,F1,F2
# to be G0,G1,G2. Note that
# G0 = (1/(4*p))*G1 - (1/(4*p))*G2,
# so that G0 is indeed a
#  linear combination of G1 and G2.
# Now we also quickly do the
# same as the above, but for the
# other version of E1 :
# yy^2 = Qu*L2u = u*(u+p)*( (1-I)*u - I*p )
# to see if it makes any
# difference to the resulting genus 2 curve.
# Again, we investigate points
# (u,yy) on E1 with u in Q and yy
# in Q(sqrt(d)) = Q(I).
Qu := u*(u+p);
L2u := (1-I)*u - I*p;
d := -1;
L2rat := u; # the rational part of Lu2
L2sqrtd := -u - p;
# the part of L2u being multiplied by sqrt(d) = I
# so that: L2u := L2rat + L2sqrtd*sqrt(d);
a := coeff(Qu,u,2);
b := coeff(Qu,u,1);
c := coeff(Qu,u,0);
# so that Qu := a*u^2 + b*u + c;
g2 := coeff(L2rat,u,1);
```

```
h2 := coeff(L2rat,u,0);
# so that L2rat := g2*u + h2;
i2 := coeff(L2sqrtd,u,1);
j2 := coeff(L2sqrtd,u,0);
# so that L2sqrtd := i2*u + j2;
# Now, let yy = r + s*sqrt(d), so that:
# (r + s*sqrt(d))^2
# = Qu*(L2rat + L2sqrtd*sqrt(d));
E1 :=
(r + s*sqrt(d))^2 - Qu*(L2rat + L2sqrtd*sqrt(d));
# so that our elliptic curve is E1 = 0.
# For this example,
# this gives: E1 := u*(u+p)*(u+I*(-u-p))
E1 := expand(E1);
# Now split E1 into its
# rational part and coeff of sqrt(d):
E1sqrtd := coeff(E1, sqrt(d));
# which corresponds to:
# 2*r*s - Qu*L2sqrtd = 2*r*s+u^3+2*p*u^2+p^2*u
# that is, the equation:
# 2*r*s = Qu*L2sqrtd. i.e. 2*r*s = -u^3-2*p*u^2-p^2*u
E1rat := expand(E1 - sqrt(d)*E1sqrtd);
# which corresponds to:
# r^2 + d*s^2 - Qu*L2rat = r^2-s^2-u^3-p*u^2
# that is, the equation:
# r^2 + d*s^2 = Qu*L2rat i.e. r^2-s^2 = u^3+p*u^2
# Now, use the first equation to solve for r:
solve(E1sqrtd,r);
# which gives: -1/2*u*(u+p)^2/s
# and substitute into the second equation:
eqna := subs(r=\%, E1rat);
# which gives:
# Qu^2*L2sqrtd^2/(4*s^2) + d*s^2 = Qu*L2rat
```

```
# eqna := Qu^2*L2sqrtd^2/(4*s^2) + d*s^2 - Qu*L2rat;
# Now let t = s^2/Qu:
eqnb := simplify(4*t*subs(s = sqrt(t*Qu), eqna)/Qu);
# which is the same as:
# L2sqrtd^2 + 4*d*t^2 = 4*L2rat*t
# eqnb := L2sqrtd^2 + 4*d*t^2 - 4*L2rat*t;
# In this example, this
# gives: p^2+2*p*u-4*t^2+u^2-4*t*u
# which is the equation:
# 4*t*u = p^2+2*p*u-4*t^2+u^2
# We want to parametrise the
# genus 0 curve eqnb as t(z),u(z).
# Rather than just letting Maple
# choose some random parametrisation,
# it's better to fix a natural
# choice of basepoint, such
# as u = root of L2sqrtd,
# t = 0, which satisfies eqnb.
eqnc :=
simplify(subs(t = L2sqrtd*z, eqnb)/L2sqrtd);
# which is the same as:
# L2sqrtd + 4*d*L2sqrtd*z^2 = 4*L2rat*z
# eqnc := L2sqrtd + 4*d*L2sqrtd*z^2 - 4*L2rat*z;
# which in this case is:
# eqnc := -p+4*p*z^2+4*z^2*u-u-4*z*u;
uz := solve(eqnc, u);
# which gives uz :=
# -p*(-1+4*z^2)/(-1+4*z^2-4*z).
# Of course, we could also have
# just used the general formula for uz
# uz := -(j2+4*z^2*d*j2-4*z*h2)
# /(i2+4*i2*z^2*d-4*z*g2);
# which gives the same answer.
```

```
tz := simplify(subs(u=uz, L2sqrtd*z));
# which gives:
# tz := 4*p*z^2/(-1+4*z^2-4*z);
# Again, we could also have
# just used our general formula:
# tz := 4*z^2*(h2*i2-g2*j2)
# /(i2+4*i2*z^2*d-4*z*g2);
# which gives the same answer.
# Check that this is a parametrisation of eqnb:
check := simplify(subs(u=uz, t=tz, eqnb));
# Our new genus 2 curve
# is then s^2 = tz*Qu(uz);
factor(simplify(tz*subs(u=uz, Qu)));
# In fact, the model is
# slightly simpler with a linear adjustment
# of z, and absorbing
# (z^2 - 8*p^2)^4/( 4*p^4*(z+2*p)^2 ) into the s^2:
(z^2 - 8*p^2)^4*factor
(subs(z= z/(4*p) + 1/2, tz*subs(u=uz, Qu)))
/( 4*p^4*(z+2*p)^2 );
# which gives the result:
# z*(z + 2*p)*(z + 4*p)*(z^2 - 8*p^2),
# which is again the same
# as the equation in the article.
# We should keep track of where
# the different factors come from:
# We should take as G0 (our new F0)
# to be the factor coming from tz:
G0 := (z^2 - 8*p^2)^2*
factor(subs(z= z/(4*p) + 1/2, tz))/( p*(z+2*p)^2 );
# which gives:
G0 := z^2 - 8*p^2;
# Now, recall that our original Qu
```

```
# factors as: u*(u+p) [of course,
# for a typical example, Qu will
# factor over a quadratic field extension].
# G1 and G2 (our new F1 and F2) are
# what arise from these factors u and u+p:
G1 := -(z^2 - 8*p^2)^2*
factor(subs(z= z/(4*p) + 1/2, subs(u=uz,u)))/p;
# which gives:
# G1 := z*(z+4*p)*(z^2 - 8*p^2);
# But z*(z + 2*p)*(z + 4*p)*(z^2 - 8*p^2)
# = square, so that
# z*(z+4*p)*(z^2 - 8*p^2)
# = (z + 2*p) mod squares, so that
# G1 mod squares and up to a constant is:
G1 := z + 2*p;
# Also:
G2 := -(z^2 - 8*p^2)^2*
factor(subs(z= z/(4*p) + 1/2, subs(u=uz,u+p)))/(4*p^2);
# which gives:
# G2 := (z + 2*p)*(z^2 - 8*p^2);
# which, modulo squares and
# up to a constant is:
G2 := z*(z + 4*p);
# So, this is a complete cycle,
# and we can take our new F0,F1,F2
# to be G0,G1,G2.
# Note that G0 = G2 - 4*p*G1,
# so that G0 is indeed a linear
# combination of G1 and G2.
# Note that the two models of
# E1 gave rise to exactly the same
# genus 2 curve:
# square = z*(z + 2*p)*(z + 4*p)*(z^2 - 8*p^2), and
```

```
# the same 3 at-most-quadratic factors: o
# z^2 - 8*p^2, z + 2*p, z*(z + 4*p).
# The only difference is that the
# first version implied that
# the choice of G0 (for the next cycle)
# should be z + 2*p,
# whereas the "systematic" approach
# suggests that G0 should be z^2 - 8*p^2.
# We'll go with the latter for the next cycle.
# At this point, we have completed
# one cycle and are ready to start
# a new cycle with F0,F1,F2 being
# the z^2 - 8*p^2, z + 2*p, z*(z + 4*p)
# obtained at the end of the last cycle.
# Now start the new cycle.
F0 := (X^2 - 8*p^2);
F1 := (X + 2*p);
F2 := X*(X + 4*p);
a0 := coeff(F0,X,2);
b0 := coeff(F0,X,1);
c0 := coeff(F0,X,0);
a1 := coeff(F1,X,2);
b1 := coeff(F1,X,1);
c1 := coeff(F1,X,0);
a2 := coeff(F2,X,2);
b2 := coeff(F2,X,1);
c2 := coeff(F2,X,0);
ResF1F2 := resultant(F1,F2,X);
# which gave: -4*p^2  which
# is the same as for the first cycle.
# Note that sqrt(ResF1F2)
# annoyingly gives 2*(-p^2)^(1/2) and
# we'd prefer p to be taken to the outside:
```

```
rr := factors(factor(resultant(F1,F2,X)));
sqrtResF1F2
:= sqrt(rr[1])*
product( (rr[2][i][1])^(iquo(rr[2][i][2],2))
*(sqrt(rr[2][i][1]))^(irem(rr[2][i][2],2)),
i = 1..nops(rr[2]));
# which gives the nicer form of the result:
sqrtResF1F2 := 2*I*p;
k1 := -(a2*c0-a0*c2)/(a1*c2-a2*c1);
k2 := (a1*c0-c1*a0)/(a1*c2-a2*c1);
k1 := expand(k1); k2 := expand(k2);
# From the formulae for these,
# this gave the result:
k1 := -4*p;
k2 := 1;
# To get tau, which swaps the
# roots of F1 and swaps the roots
# of F2, we use the formula
tau := ((a1*c2-a2*c1)*X + b1*c2-b2*c1)
/((a2*b1-a1*b2)*X + a2*c1-a1*c2);
tau := factor(tau);
# and it gives tau := -2*p*(X+4*p)/(X+2*p).
# And from the formula for sigma we get
sigma := (X + 2*p + 2*I*p)/(X + 2*p - 2*I*p);
# Also apply the general formula for the inverse of sigma:
sigmainv
:= -((a1*c2 - a2*c1)*(T-1) + sqrtResF1F2*(T+1) )/
( (a1*b2 - a2*b1)*(T-1) );
sigmainv := simplify(sigmainv);
# which gives: sigmainv := 2*p*(-T+I*T+1+I)/(T-1);
# Now, focus on the 3 curves relating to the identity:
# EE0 : Y^2 = F1*F2 = (X + 2*p)*X*(X + 4*p),
# EE1 : Y^2 = F0*F2 = (X^2 - 8*p^2)*X*(X + 4*p),
```

```
# EE2 : Y^2 = F0*F1 = (X^2 - 8*p^2)*(X + 2*p).
# The first of these is an elliptic curve over Q.
# It's rank is relevant
# (if the rank is 0, then the method is
# immediately successful in
# excluding this case), but is
# not needed for constructing
# the next genus 2 curve
# (which only involves EE1,EE2).
# Note that d=1 now, so
# that Q(sqrt(d)) is just Q.
# We first need to map EE1,EE2
# to elliptic curves E1,E2 of the form:
# square = (quadratic over Q)*(linear over Q),
# and such that the map on
# the x-coordinate is Q-rational.
F0T :=
subs(X = sigmainv, F0);
F0T :=
factor(expand(simplify(F0T)))*(T - 1)^2;
F1T :=
subs(X = sigmainv, F1);
F1T :=
factor(expand(simplify(F1T)))*(T - 1)^2;
F2T :=
subs(X = sigmainv, F2);
F2T :=
factor(expand(simplify(F2T)))*(T - 1)^2;
# These gave:
# F0T := (-8-8*I)*(T^2-I)*p^2;
# F1T := 2*I*p*(T^2-1);
# F2T := -8*p^2*(T^2+1);
# At this point, we have only
```

```
# even-power terms in T
F0x := subs(T = sqrt(x), F0T);
F1x := subs(T = sqrt(x), F1T);
F2x := subs(T = sqrt(x), F2T);
# .. which means that EE1 maps
# under (X,Y) |-> (sigma^2, sigma*Y*(sigma-1)^3)
# to: square = 64*(1+I)*p^4*x*(x-I)*(x+1)
# which simplifies to:
# square = (1+I)*x*(x-I)*(x+1)
# and EE2 maps under the same map to:
# square = 16*(1-I)*p^3*x*(x-I)*(x-1)
# which simplifies to:
# square = (1-I)*p*x*(x-I)*(x-1)
# However, the x-coordinate map
# X |-> x = sigma^2 is not Q-rational, and
# so we need a further mobius
# transformation to map it Q-rational.
# We need the further mobius transformation
# to give v, which is Q-rational.
# The general case tells us
# we should now change from x to v where:
# v := sqrt(d*ResF1F2)*(x+1)/(x-1),
# where d = 1 and ResF1F2 = -4*p^2,
# so that sqrt(d*ResF1F2) = 2*p*I, so that:
# v := 2*p*I*(x+1)/(x-1)
# which has inverse x := (v+2*p*I)/(v-2*p*I);
# We now see that:
# square = (1+I)*x*(x-I)*(x+1) becomes:
subs( x = (v+2*p*I)/(v-2*p*I),
(1+I)*x*(x-I)*(x+1) );
# We can multiply through by
# (1/4)*(v - 2*I*p)^4, which is square and so
# can be absorbed into y^2:
```

```
E1v := factor(\%*(v-2*I*p)^4)/4;
# This gave the result:
# (v+2*I*p)*(v-2*I*p)*(v-2*p)*v
# where the linear factor v-2*p
# arose from x - I
# [as can be seen from numer of
# factor(subs(x=(v+2*p*I)/(v-2*p*I),(x-I)))]
# which in turn arose from
# F0 = X^2 - 8*p^2. The general strategy
# tells us that we should first
# find v0, the root of this factor:
v0 := solve(v-2*p,v);
# which of course gives v0 := 2*p;
# and now we map to u = 1/(v-v0),
# with inverse v = v0 + 1/u,
# which has the effect
# of mapping (v0,0) to infinity:
factor( expand(subs(v = v0 + 1/u, E1v)) );
# which gave the result:
#  4*(2*p*u+1)*(8*p^2*u^2+1+4*p*u)/u^4
# We also multiply through by
# u^4, which gets absorbed into the y^2:
\%*u^4;
# .. and a linear change in
# u takes it to a nicer form:
factor(subs(u = (u-p)/(4*p^2), \%))*4*p^4;
# which gives: E1: square = (u^2+p^2)*p*(u+p)
# Similarly E2: square = (1-I)*p*x*(x-I)*(x-1)
# We now see that:
# square = (1-I)*p*x*(x-I)*(x-1) becomes:
subs( x = (v+2*p*I)/(v-2*p*I),
(1-I)*p*x*(x-I)*(x-1));
# We can multiply through by
```

```
# (v - 2*I*p)^4, which is square and so
# can be absorbed into y^2:
E2v := factor(\%*(v-2*I*p)^4);
# This gave the result:
# (v+2*I*p)*(v-2*I*p)*(v-2*p)*8*p^2
# where the linear factor v-2*p arose from x - I
# [as can be seen from numer of
# factor(subs(x=(v+2*p*I)/(v-2*p*I),(x-I)))]
# which in turn arose from
# F0 = X^2 - 8*p^2. The general strategy
# tells us that we should first
# find v0, the root of this factor:
v0 := solve(v-2*p,v);
# which of course gives v0 := 2*p;
# and now we map to u = 1/(v-v0),
# with inverse v = v0 + 1/u,
# which has the effect of mapping (v0,0) to infinity:
# factor( expand(subs(v = v0 + 1/u, E2v)) );
# N.B. We are required now
# to perform the same linear change on u
# for E2 that we did for E1
# (so that u means the same thing in both cases).
# .. and a linear change in
# u takes it to a nicer form:
simplify( factor
(subs(u = (u-p)/(4*p^2), \%))*(u-p)^4/256/p^6 );
# giving: E2: square = (u^2+p^2)*(u-p)
# Here, the u^2 + p^2
# is the quadratic common to E1,E2 and
# the p*(u+p) and the u-p
# are the linear factors for E1,E2, resply.
# The u^2 + p^2 is our Qu,
# and the p*(u+p) and u-p are the
```

```
# "conjugate" linear factor over Q(sqrt(d)) = Q.
# Now go to step 2.
Qu := u^2 + p^2;
L2u := p*(u+p);
d := 1;
# We now want to compute
# L2rat and L2sqrtd such that
# L2u := L2rat + L2sqrtd*sqrt(d)
# = L2rat + L2sqrtd;
# We know that L1u := u-p =
# L2rat - L2sqrtd*sqrt(d) = L2rat - L2sqrtd;
# so that:
L1u := u-p;
L2rat := expand( (L2u + L1u)/2 );
L2sqrtd := expand( (L2u - L1u)/2 );
# so that:
# L2u := L2rat + L2sqrtd*sqrt(d);
a := coeff(Qu,u,2);
b := coeff(Qu,u,1);
c := coeff(Qu,u,0);
# so that Qu := a*u^2 + b*u + c;
g2 := coeff(L2rat,u,1);
h2 := coeff(L2rat,u,0);
# so that L2rat := g2*u + h2;
i2 := coeff(L2sqrtd,u,1);
j2 := coeff(L2sqrtd,u,0);
# so that L2sqrtd := i2*u + j2;
# Now, let yy = r + s*sqrt(d), so that:
# (r + s*sqrt(d))^2
# = Qu*(L2rat + L2sqrtd*sqrt(d));
E1 := (r + s*sqrt(d))^2 -
Qu*(L2rat + L2sqrtd*sqrt(d));
# so that our elliptic curve is E1 = 0.
```

```
# For this example,
# this gives: E1 := (r+s)^2-(u+p)*(u^2+p^2)*p
E1 := expand(E1);
# Now split E1 into its
# rational part and coeff of sqrt(d):
E1sqrtd := 2*r*s - Qu*L2sqrtd;
# which corresponds to: 2*r*s - Qu*L2sqrtd
# that is, the equation: 2*r*s = Qu*L2sqrtd.
E1rat := expand(E1 - sqrt(d)*E1sqrtd);
# Now, use the first equation to solve for r:
solve(E1sqrtd,r);
# which gives: -1/2*u*(u+p)^2/s
# and substitute into the second equation:
eqna := subs(r=\%, E1rat);
# which gives:
# Qu^2*L2sqrtd^2/(4*s^2)
# + d*s^2 = Qu*L2rat
# eqna := Qu^2*L2sqrtd^2/(4*s^2)
# + d*s^2 - Qu*L2rat;
# Now let t = s^2/Qu:
eqnb := simplify(4*t*
subs(s = sqrt(t*Qu), eqna)/Qu);
# which is the same as:
# L2sqrtd^2 + 4*d*t^2 = 4*L2rat*t
# eqnb := L2sqrtd^2 + 4*d*t^2 - 4*L2rat*t;
# We want to parametrise the
# genus 0 curve eqnb as t(z),u(z).
# Rather than just letting Maple
# choose some random parametrisation,
# it's better to fix a
# natural choice of basepoint, such
# as u = root of L2sqrtd,
# t = 0, which satisfies eqnb.
```

```
eqnc :=
simplify(subs(t = L2sqrtd*z, eqnb)/L2sqrtd);
# which is the same as:
# L2sqrtd + 4*d*L2sqrtd*z^2 = 4*L2rat*z
# eqnc := L2sqrtd + 4*d*L2sqrtd*z^2 - 4*L2rat*z;
# which in this case is:
# eqnc := -p+4*p*z^2+4*z^2*u-u-4*z*u;
uz := solve(eqnc, u);
# which gives uz :=
# -p*(4*p*z^2+p-4*z*p+1+4*z^2+4*z)
#/(-4*z*p+4*p*z^2+p-4*z^2-1-4*z)
# Of course, we could also have
# just used the general formula for uz
# uz := -(j2+4*z^2*d*j2-4*z*h2)
#/(i2+4*i2*z^2*d-4*z*g2);
# which gives the same answer.
tz := simplify(subs(u=uz, L2sqrtd*z));
# which gives:
# tz := -8*z^2*p^2
# /(-4*z*p+4*p*z^2+p-4*z^2-1-4*z);
# Again, we could also have
# just used our general formula:
# tz := 4*z^2*(h2*i2-g2*j2)
# /(i2+4*i2*z^2*d-4*z*g2);
# which gives the same answer.
# Check that this is a parametrisation of eqnb:
check := simplify(subs(u=uz, t=tz, eqnb));
# Our new genus 2 curve is then s^2 = tz*Qu(uz);
factor(simplify(tz*subs(u=uz, Qu)));
# But in any case, recall that we are just looking for
# genus 2 curve which maps to both of:
# E1 : square = (u^2+p^2)*p*(u+p)
# E2 : square = (u^2+p^2)*(u-p)
```

```
# Clearly this is achieved by:
# C : Y^2 = (X^4 + p^2)*(X^2 - p),
# since the map (X,Y) |-> (X^2,Y) is from this curve
# to E2, and the map (X,Y) |-> (-p^2/X^2, p*Y/X^3)
# So, after starting with
# Y^2 = (X^4 + p^2)*(X^2 + p) and
# performing two cycles,
# we get Y^2 = (X^4 + p^2)*(X^2 - p).
# Of course, geometrically
# we are now back to the original
# curve, since (X,Y) |-> (I*X, I*Y)
# is a birational transformation
# between Y^2 = (X^4 + p^2)*(X^2 + p)
# and Y^2 = (X^4 + p^2)*(X^2 - p).
# So, after two complete cycles,
# we get back to a curve
# which is birationally equivalent
# over Q(I), but not over Q.
# Note also that we never used
# (in any of the above) that
# p is prime. All of the above
# work for p being any rational number.
# Note also that the final
# curve is the same as the starting
# curve, but with p replaced
# by -p. If we let pp denote -p,
# then are after-2-cycles curve
# is: Y^2 = (X^4 + pp^2)*(X^2 + pp).
# So, a further 2 cycles will
# take it to: Y^2 = (X^4 + pp^2)*(X^2 - pp)
# which is just: Y^2 = (X^4 + p^2)*(X^2 + p).
# So, repetition must occur in 4 cycles!
```

B.1.4 Magma code relating to Selmer bound computations in Chapters 4,5

```
#Here I describe the commands used in Magma
#to show that for the curve
#(x^2+p)(x^4+p^2) and its similar curves
#(ie. those in the cycle), that the
#Selmer bounds will evade both
#Chabauty, this method etc.
#For p=31, all commands are given.
#For p=47 and p=79,
#just replace 31 in all the curves below
#The first curve we
#consider is $(x^2+31)(x^4+31^2)$.
P<x> := PolynomialRing(Rationals());
C1 := (x^2+31)*(x^4+31^2);
Jac1 := Jacobian(HyperellipticCurve(C1));
SetVerbose("JacHypSelmer",1);
TwoSelmerGroupData(Jac1);
#This command provides the Selmer bound as $2$.
#For the next genus two curve in the cycle we look at
# (x^2-8*p^2)*(x+2*p)*x*(x+4*p) where p=31
# We imitate the above Magma commands.
P<x> := PolynomialRing(Rationals());
C2 := (x^2-(8*31*31))*(x+(2*31))*(x+(4*31))*x;
Jac2 := Jacobian(HyperellipticCurve(C2));
SetVerbose("JacHypSelmer",1);
TwoSelmerGroupData(Jac2);
#Here we get the rank bound of $2$.
#The next curve is just the first with 31 replaced by -31.
#The commands are thus...
P<x> := PolynomialRing(Rationals());
C3 := (x^2-31)*(x^4+(-31)^2);
```

```
Jac3 := Jacobian(HyperellipticCurve(C3));
SetVerbose("JacHypSelmer",1);
TwoSelmerGroupData(Jac1);
#Here we get Selmer bound of $3$.
#The final curve commands will be
P<x> := PolynomialRing(Rationals());
C4 := (x^2-(8*(-31)*(-31)))*(x+(2*(-31)))*(x+(4*(-31)))*x;
Jac4 := Jacobian(HyperellipticCurve(C4));
SetVerbose("JacHypSelmer",1);
TwoSelmerGroupData(Jac4);
#Here we get rank bound of $2$.
```

B.1.5 Apecs commands relating to Selmer bound computations in Chapters 4,5

```
#Now we need to check the elliptic curves.
#Commands below are for Apecs.
#First cycle is: y^2 = x*(x^2 + 31^2)
Ein(0,0,0,31^2,0);
RkNC();
#Unconditionally rank 1 with point
#of infinite order, found by the command >RR;

# Second cycle is: y^2 = (x + 2*31)*x*(x + 4*31)
Ein(0,186,0,7688,0);RkNC();
#Unconditionally rank 1
#Third cycle is: y^2 = x*(x^2 + 17^2)
#This is exactly the same as the first curve
#Fourth cycle gives: y^2 = (x - 2*31)*x*(x - 4*31)
Ein(0,-186,0,7688,0);
RkNC();
```

Bibliography

[1] A. Agashe and W. Stein. Visibility of Shafarevich-Tate groups of abelian varieties. *J. Number Theory* **97** (2002), 171–185.

[2] A. Bremner, D.J. Lewis and P. Morton. Some varieties with points only in a field extension. *Arch. Math.* **43** (1984), 344–350.

[3] D.G. Cantor. Computing in the Jacobian of a Hyperelliptic curve. *Math. Comp.* **48** (1987), 95–101.

[4] J.W.S. Cassels. The arithmetic of certain quartic curves. *Proc. Royal Soc. Edinburgh* **100A** (1985), 201–218.

[5] J.W.S. Cassels. Local Fields. London Mathematical Society Student Texts, No. 3 (1986). Cambridge University Press.

[6] J.W.S. Cassels. *Lectures on elliptic curves.* London Mathematical Society Student Texts **24** (1991), Cambridge University Press.

[7] J.W.S. Cassels. On a Theorem of Dem'janenko. *J. London Math. Soc.* **43** (1968), 61–66.

[8] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2.* London Mathematical Society Lecture Note Series **230** (1996), Cambridge University Press.

[9] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci. Paris* **212** (1941), 882–885.

[10] V. Dem'janenko. Rational points of a class of algebraic curves. *Trans. Amer. Math. Soc.* **66** (1968), 246–272.

[11] G. Faltings. *Rational Points.* Friedrich Vieweg & Sons, 1992.

[12] E.V. Flynn. The group law on the Jacobian of a curve of genus 2. *J. reine angew. Math.* **439** (1993), 45–69.

[13] E.V. Flynn. Descent via isogeny in dimension 2. *Acta Arith.* **LXVI.1** (1994), 23–43.

[14] E.V. Flynn. On a Theorem of Coleman. *Manuscripta Math.* **88** (1995), 447–456.

[15] E.V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Mathematica* **105** (1997), 79–94.

[16] E.V. Flynn. Coverings of Curves of Genus 2. Algorithmic Number Theory, Wieb Bosma, ed. *Lecture Notes in Computer Science* **1838** (2000), 65–84. Springer-Verlag.

[17] E.V. Flynn and J. Redmond. Application of covering techniques to families of curves. *J. Number Theory* **101** (2003), 376–397.

[18] E.V. Flynn and N.P. Smart. Canonical heights on the Jacobian of curves of genus 2 and the infinite descent. *Acta Arithmetica* **LXXIX.4** (1997), 333–352.

[19] E.V. Flynn and J.L. Wetherell. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.* **100** (1999), 519–533.

[20] E.V. Flynn and J.L. Wetherell. Covering collections and a challenge problem of Serre. *Acta Aritmetica* **XCVIII.2** (2001), 197–205.

[21] G. Frey and E. Kani. Curves of genus 2 covering elliptic curves and an arithmetical application. Arithmetic Algebraic Geometry, G. van der Geer, F. Oort and J. Steenbrink, eds., *Progress in Mathematics* 89 (1991), 153–175. Birkhäuser, Boston.

[22] J.R. Merriman and N.P. Smart. Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point. *Math. Proc. Camb. Phil. Soc.* **114** (1993), 203–241.

[23] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. Progress in Math. **94** (1991), Birkhäuser, Boston, pp. 313–334.

[24] R.A. Mollin. *Algebraic number theory* (1999). Chapman and Hall/CRC.

[25] D. Mumford. *Curves and their Jacobians* (1975). University of Michigan Press.

[26] I.N. Stewart and D.O. Tall. *Algebraic Number Theory* (1979). Chapman and Hall.

[27] J.-P. Serre. *Lectures on the Mordell-Weil Theorem* (1989). Transl. and ed. by Martin Brown. ¿From notes by Michel Waldschmidt. Vieweg.

[28] E.F. Shaefer. Computing a Selmer group of a Jacobian using functions on a curve. *Math. Ann.* **310** (1998) no. 3, 447–471.

[29] J.H. Silverman. The arithmetic of elliptic curves (1986). Springer-Verlag.

[30] J.H. Silverman. Advanced topics in the arithmetic of elliptic curves (1994). Springer-Verlag.

[31] H.P.F. Swinnerton-Dyer. *A brief guide to algebraic number theory.* London Mathematical Society Student Texts **50** (2001). Cambridge University Press.

[32] R. Walker. *Algebraic Curves* (1962). Dover.

[33] J. Wetherell Bounding the number of rational points on certain curves of high rank. PhD dissertation (1997), University of California at Berkeley.

[34] A. Weil. L'arithmetique sur les courbes algebriques. *Acta Math.* **52** (1929), 281–315.

[35] A. Weil. Remarques sur un memoire d'Hermite. *Arch. d. Math.* **5** (1954), 197–202.

[36] H.G. Zimmer. Basic algorithms for elliptic curves. *Proceedings Number Theory, Eger, 1996* Gruyter (1998), 541–595.

[37] *The Elliptic curve handbook*, available from:

ftp://ftp.math.mcgill.ca/pub/ECH1/

[38] *Apecs*, designed by Ian McConnell available from:

ftp://ftp.math.mcgill.ca/pub/apecs/Apecs6/

[39] *Maple Version 9*, designed by and available from:

http://www.maplesoft.com/

[40] *The Magma computational algebra system*, produced and distributed by the Computational Algebra Group within the School of Mathematics and Statistics of the University of Sydney, available at:

http://magma.maths.usyd.edu.au/magma/